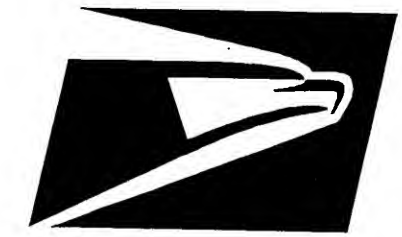
DRAFT

# PERFORMANCE CRITERIA FOR INFORMATION-BASED INDICIA PROGRAM (IBIP) SYSTEMS EMPLOYING CENTRALIZED POSTAL SECURITY DEVICES




®

August 17, 2000

# TABLE OF CONTENTS

# 1. INTRODUCTION

The United States Postal Service (USPS) initiated the Information-Based Indicia Program (IBIP) to enhance security of postage evidencing and to support new methods of applying postage to mail. This document, *Performance Criteria for Information-Based Indicia Program (IBIP) Systems Employing Centralized Postal Security Devices (PSDs)*, defines the requirements for the Wide Area Network (WAN) elements of IBIP. This system is different from the original IBIP concept in the way that a user interacts with both the Product Service Provider (i.e., "Provider") and the USPS. Unlike the original concept, in which users were expected to use dedicated hardware along with a computer to interact with the Provider and the USPS, the IBIP WAN System allows multiple users to access a single centralized Postal Security Device (PSD) site when interacting with the Provider and the USPS.

## 1.1. Structure of Performance Criteria

This document is composed of five major parts: Indicium, Postal Security Device, Centralized PSD Site, Client System, and IBIP Key Management. It organizes relevant IBIP performance criteria needed for a Provider to participate in the IBIP WAN System. The following overview describes each of the chapters:

- **Chapter 2 — IBIP WAN System Overview:** This chapter introduces the components and the participants of the IBIP WAN System and describes how the systems are configured.
- **Chapter 3 — Indicium:** This chapter defines the requirements for the indicium (i.e., postage mark) to be applied to mail produced by the IBIP WAN System.
- **Chapter 4 — Postal Security Device (PSD):** This chapter defines the requirements for a PSD that will provide security services to support the creation of the new indicium to be applied to mail using the IBIP WAN System.
- **Chapter 5 — Centralized PSD Site:** This chapter defines the requirements for a centralized site that will house the PSD and interact with the IBIP WAN System.
- **Chapter 6 — Client System:** This chapter describes the performance criteria for the user's client system that supports the IBIP WAN System.
- **Chapter 7 — Key Management:** This chapter of the performance criteria document describes the key registration process and attributes of the keys used in the IBIP digital signatures.

## 1.2. Interpretation of Requirements

The requirements presented in this document are composed of statements containing the words "shall" or "must." Requirements using the words "shall" or "must" are mandatory. Other statements use the words "should" or "may." Statements using the words "should" are recommendations; statements using the words "may" are design-related or functional options to consider for implementation purposes.

## 1.3. Year 2000 Compliance

All components of a system used to produce information-based indicia shall be year 2000 compliant. "Year 2000" compliant means that the system shall accurately process date and time data (including, but not limited to, calculating, comparing, and sequencing) for

the year 2000, for the twenty-first century, and for leap year calculations. The system shall properly exchange data and time data with other systems with which it must interface to meet the performance criteria.

### 1.4. Reference Documents and Resources

The proposed requirements and performance criteria included in this document are supported by a number of published resources. The primary resources supporting this document are the following:

- "Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBIO)," February 23, 2000.
- "Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C)," Draft January 12, 1999.
- Federal Register, Vol. 63, No. 170, pages 46719-46728, September 2, 1998, "Proposed Rule on Manufacture, Distribution, and Use of Postal Security Devices and Information-Based Indicia," 39 CFR Parts 111 and 502.
- USPS *Domestic Mail Manual* (DMM), Issue 55, January 10, 2000.
- USPS *International Mail Manual* (IMM), Issue 21, July 1, 2000.
- "Uniform Symbology Specification PDF417," July 1994.
- "Digital Signature Standard — FIPS PUB 186," May 19, 1994, and Change 1, December 1, 1996.
- "Secure Hash Standard — FIPS PUB 180-1," April 17, 1995.
- "PKCS #1: RSA Encryption Standard," Version 1.5, December 1, 1993.
- "ANSI X9.62, Elliptic Curve Digital Signature Algorithm Standard (ECDSA)," Working Draft, January 15, 1997.
- "Security Requirements for Cryptographic Modules — FIPS PUB 140-1," January 11, 1994.
- "Cryptographic Module Validation Program Announcement," July 17, 1995.
- "Coding Accuracy Support System, AMS-II, Technical Guide," March 1996.
- "ISO/IEC 9594-8 (1995). Information Technology — Open Systems Interconnection — The Directory: Authentication Framework."
- "PKCS #10: Certification Request Syntax Standard, An RSA Laboratories Technical Note," Version 1.0, December 1993.
- USPS Publication 25, *Designing Letter Mail*, June 2000.
- "Directory Authentication Framework Recommendation X.509."

### 1.5. Intellectual Property and License Considerations

Providers who choose to produce a postage evidencing product or service must comply with USPS Intellectual Property (IP) Requirements as a condition for receiving and maintaining regulatory approval. If a Provider is unable or unwilling to meet the IP requirements, it should not offer the product or service.

Providers do not have authorization or consent from the USPS under 28 U.S.C. 1498(a) or otherwise to make or use any patented invention.

The USPS reserves the right and authority to discontinue a Provider's authorization to distribute a postage evidencing device or service if the USPS or a court determines that the manufacture of the device or service, the use of the device or service by mailers, or the validation of the indicia produced by the device or service requires use of patented inventions for which the Provider has not procured appropriate licenses.

This requirement applies to all aspects of the Provider's product or service, including those required or specified under applicable performance criteria.

# 2. IBIP WAN SYSTEM OVERVIEW

The IBIP WAN System concept is an alternative to the original IBIP concept, which envisioned a system in which a client computer, PSD, and printer would be physically collocated so that the entire postage printing operation was under the physical control of the user. The alternative IBIP WAN concept is configured so that multiple client computers have access to a Provider-operated, centralized PSD site through a communications network such as the Internet.

## 2.1. System Components

The IBIP WAN System consists of the following components: indicium, client system, and PSD. Each of these components is defined below with a brief description of its function within the IBIP WAN System.

### 2.1.1. Indicium

The indicium is the physical postage mark that is printed and applied to mail. The indicium contains a two-dimensional barcode in addition to human-readable information. The information in the indicium contains a variety of mail-processing data requirements and security-related information. The indicium contains a digital signature to prevent forgery and ensure uniqueness and authenticity.

### 2.1.2. Client System

The client system is a combination of the processor running the appropriate software application that provides overall control of the mailpiece production process and a printer used to physically produce indicia. The processor includes an operator interface so that a user may input various parameters to customize the mailpiece (e.g., postage amount, date of mailing, destination ZIP Code, etc). The user operates the client system to interact with the Provider and the Postal Security Device (PSD) when requesting and receiving indicia.

### 2.1.3. Postal Security Device (PSD)

The PSD is the main component of the centralized PSD site that communicates with all of the participants in the IBIP WAN System. The PSD is composed of a FIPS-approved cryptographic subsystem and a repository of revenue sensitive register values. The cryptographic subsystem performs the core security functions in this system by utilizing encryption functions that ensure that data transferred between the PSD and its interfaces are safe and not threatened by attacks. The repository of revenue sensitive register values maintains the amount of money that individual users accessing the PSD have to purchase and produce indicia.

These components are the pieces that are necessary to form a complete postage evidencing and printing system. In the IBIP WAN System, these components will be connected in a manner in which the client and printer will be separated from the PSD. The PSD will be located at a centralized site so it will be accessible to multiple users and clients trying to produce indicia.

## 2.2. IBIP WAN Participants

In the IBIP WAN System, the user, the Provider, and the USPS interact with each other to allow users to produce indicia. In this system, the PSD is located at a central location, thus alleviating the need to have individual PSDs at every user's client system site. In the IBIP WAN System, users contact the centralized PSD site, which is operated by the Provider, to request indicia. The USPS regulates and oversees the interaction between the user and the Provider while at the same time interacting with both the user and Provider.

### 2.2.1. User

The role of the user in the IBIP WAN System is to install the appropriate software for use on the client system computer. The choice of software will depend on the user's choice of Provider. Once this has been completed, the user will then be able to use the client system computer and software to submit valid registration information with the Provider to obtain a user registration from the Postal Service. Through the Provider, the user will also supply funds that will be deposited with the USPS Treasury in order to request and print indicia. Finally, the user will use his or her client system, consisting of a PC and printer, to print out indicia for application onto mailpieces.

### 2.2.2. Provider

The role of the Provider is essential in the IBIP WAN System. The Provider will operate the centralized PSD site that performs the core security functions in the system. The Provider will first develop and obtain approval for its software and PSD. The software created by the Provider will have user registration capabilities. The Provider is also responsible for an auditing procedure that will keep track of user indicia production. This is required to protect the USPS revenue since a record of user transactions must exist in case the PSD fails and the Provider has to reload backup information. The Provider also will perform analysis on pieces of submitted mail to ensure the quality and readability of indicia, in accordance with the Mailpiece Quality Assurance Program. Finally, the Provider will act as an interface between the USPS, the USPS Treasury, and the USPS Certification Authority. The interaction between the Provider and the USPS is primarily to ensure that logical security elements are maintained. The Provider and the USPS Treasury interact so that the appropriate funds can be deposited, thus allowing users to be able to print indicia. The USPS Certification Authority deals with the Provider to enable authentication on any electronic transactions between the USPS, Providers, and users.

### 2.2.3. USPS

The primary role of the USPS in the context of the IBIP WAN System is to assure that postal revenues passing through such a system are protected. The USPS has a variety of functions in this system. First, the USPS controls the issuance of user registrations. Users who want to print indicia are required to register and be approved by the Postal Service before they are permitted to use the services of any Provider. The USPS shall also grant approval to the Provider with regards to the Provider's registration methodology, software, and PSD. A critical function of the USPS in protecting its revenue is to monitor any irregularities that might arise in interactions between any of the single entities of the IBIP WAN System. If any irregularities are found, the USPS must contact the Provider and/or the user to determine the cause of these irregularities.

The role of the USPS Treasury is to collect and account for the money that is paid by the users of the IBIP WAN System. A user sends an indicia request to the centralized PSD site. If sufficient funds are on deposit and the request is granted, the register values for the user will change accordingly. It is the responsibility of the USPS Treasury to audit the records of the Provider to certify that a user's deposited funds equal the sum of the register values at the centralized PSD site.

## 2.3. System Configuration

The IBIP WAN System is configured so that a centralized PSD site can service multiple users as opposed to a single user in the original IBIP system. As a result, the IBIP WAN System has both a centralized PSD and a Provider site that are accessible to the user and client system through public and/or private networks. The resources of these private networks are protected by individual firewalls. The firewall at the interface for the Provider site and the client protects important registration information that the user supplies. The firewall at the interface for the centralized PSD site and the client protects information pertaining to register values and other transactions. Figure 2-1 depicts a generalized configuration for the IBIP WAN System.

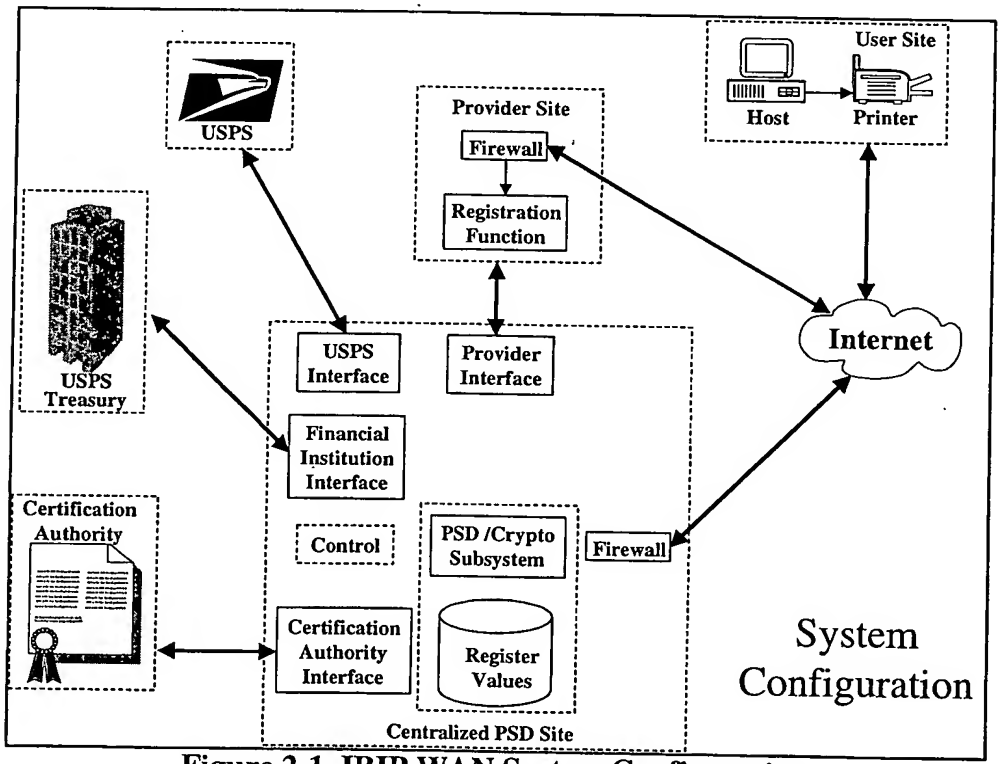



**Figure 2-1. IBIP WAN System Configuration**

As shown in Figure 2-2, the user in the IBIP WAN System interacts directly with the Provider and the Provider-operated centralized PSD site. The primary responsibilities of the user are to register with the Provider, deposit money with the USPS Treasury, and request indicia from the centralized PSD site so he or she may produce indicia using the user's client system. The user must first submit registration information to the Provider who will then forward it to the USPS. The USPS will review this information and, through the Provider, will grant the user approval for indicia production if all registration criteria are met. After the user has deposited money with the USPS Treasury, the user may then request indicia from the centralized PSD site. The PSD will respond to the indicia request by checking to see if the user has sufficient funds deposited. If sufficient funds are on deposit, the indicia data will be sent back to the user.

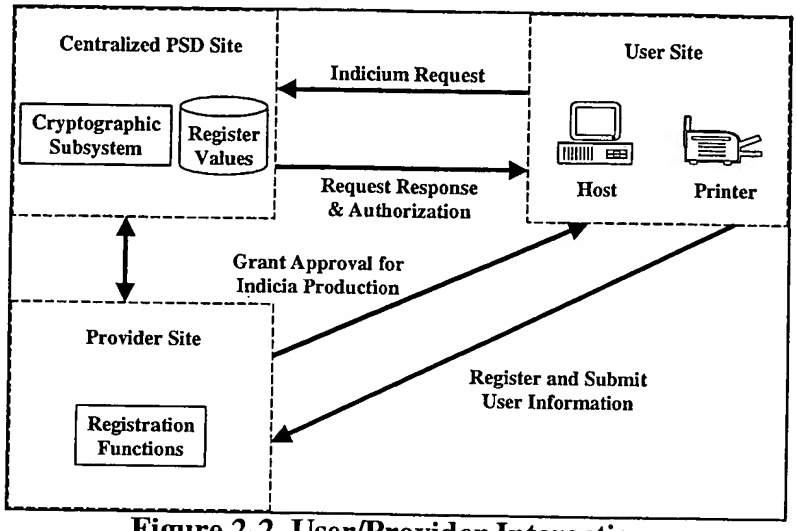



**Figure 2-2. User/Provider Interactions**

The primary role of the USPS in the IBIP WAN System is to protect its revenue from any fraudulent activity. The USPS interacts with the Provider to obtain user registration information. The USPS reviews the information submitted by the user and then determines whether to grant a user registration that would allow use of a postage evidencing and printing system. This interaction between the USPS and the Provider is depicted in Figure 2-3.

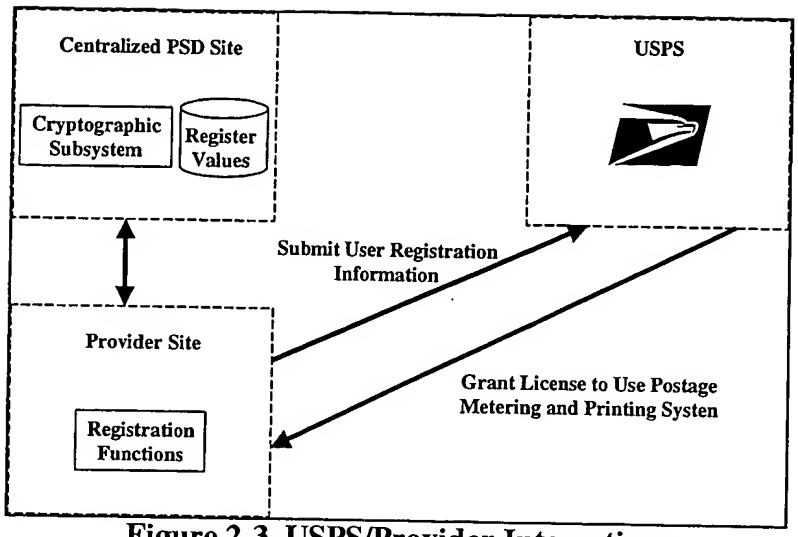



**Figure 2-3. USPS/Provider Interactions**

The method of payment by the user in the IBIP WAN System is depicted in Figure 2-4. Before a user may print indicia, sufficient funds must be deposited. The user can deposit funds by providing credit card authorization for a certain monetary value. The Provider in turn will interact with a credit card processor to determine if approval can be granted on such a transaction. Once approval has been obtained, the Provider will notify the USPS of funds deposited by the user. The user is now able to print indicia. Each time indicia are printed by the user, the register values for the user will change accordingly. The USPS Treasury will then ensure that the record of register values for each user matches the amount of funds deposited by the user

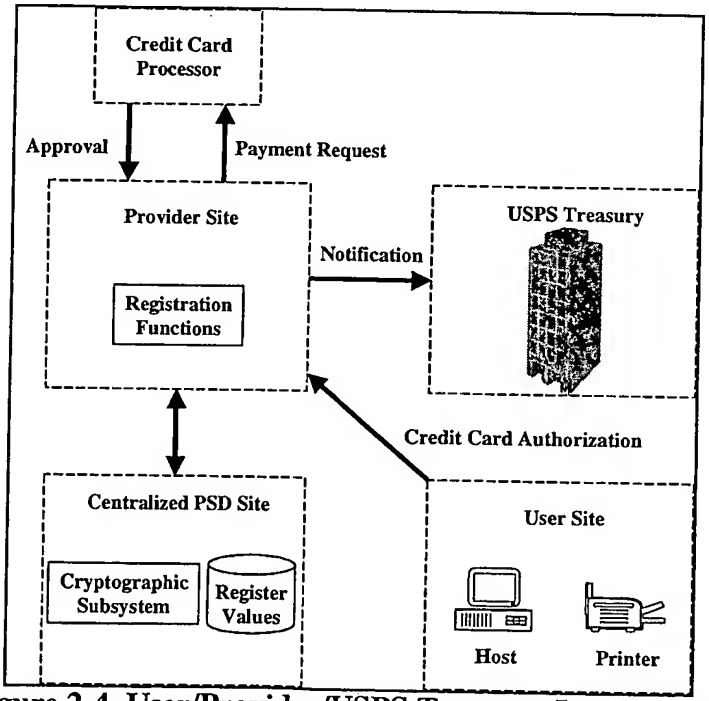
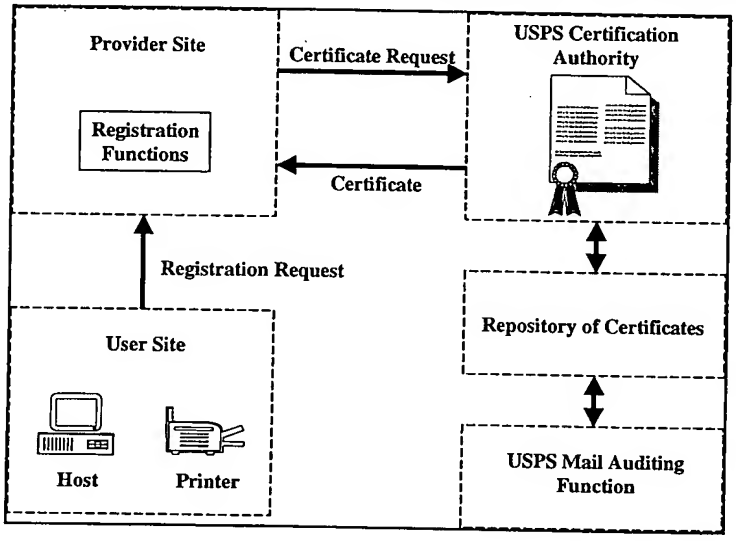



**Figure 2-4. User/Provider/USPS Treasury Interactions**

The USPS Certification Authority interacts with the Provider to certify that all electronic transactions made in the IBIP WAN System are authentic. In the IBIP, digital signatures are employed in creating indicia, in allocating postage value downloads to PSDs, in auditing postage usage, and in auditing mail bearing IBI. The USPS Certification Authority will digitally sign certificates for any party in the IBIP WAN System that is involved in one of the operations just described. These certificates will be signed using a USPS Certification Authority private key. Thus, for any transactions within the IBIP WAN System, two parties will exchange certificates with one another, and to ensure the authenticity and integrity of the material they are receiving, they can verify the signature of the USPS Certification Authority by using the Certification Authority's public key. Thus, the parties can be assured that their transactions are secure from either intentional or accidental modification. A diagram depicting the configuration of the USPS Certification Authority in the IBIP WAN System is shown in Figure 2-5.

**Figure 2-5. User/Provider/USPS Certification Authority Interactions**



# 3. INDICIUM PERFORMANCE CRITERIA

The indicium shall consist of a two-dimensional (2-D) barcode and certain human-readable information. The barcode format for the indicium shall be the PDF417 barcode or any other USPS-approved 2-D barcode standard. The information required in the barcode and in the human-readable portions of the indicium follows. Providers have some flexibility in the appearance of the indicium, provided the basic requirements contained in these performance criteria are satisfied.

The indicium provides the following features:

- Printing Technology Alternatives. The indicium supports a number of printing technology alternatives (e.g., laser, inkjet, thermal).
- Machine Readable. Through the use of a 2-D barcode, the indicium shall be readable using automated equipment.
- Standard Ink. The indicium may be printed using standard black ink or toner, provided it meets the reflectance standards defined in 3.4.6.
- Fraud Mitigation. The indicium supports various fraud mitigation strategies that are incorporated into the overall IBIP security architecture.
- Support for Future Services. The indicium offers the flexibility to provide support for new services that the USPS may offer in the future.

The IBIP supports applying postage with methods that involve the use of the client system and a printer to create and print unique indicia on mailpieces, envelopes, or labels.

## 3.1. Standard Indicium Data Contents

This section details the data contents of the indicium as described in the USPS document entitled "Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBIO)," February 23, 2000.

The standard indicium shall consist of both human-readable and barcode data. The human-readable information shall show the minimum information as specified in the DMM. The barcoded information shall meet the requirements for the IBI specified in this section. The following paragraphs detail the data elements included in the indicium. The formats, output characteristics, and order of the data elements within the indicium are specified in Table 3-1. Two additional indicia types that the user may print to address special cases are Redate and Postage Correction indicia. The data content for these special-purpose indicia is discussed in 3.2. Barcode data shall include machine-readable ASCII format data, as well as binary format data for the digital signature.

USPS intends to support multiple cryptographic digital signature algorithms. As necessary to support Provider implementations, the USPS supports use of the Digital Signature Algorithm (DSA), Rivest Shamir Adleman (RSA) Algorithm, and Elliptic Curve Digital Signature Algorithm (ECDSA) systems to generate the digital signature for the indicium. The length of the digital signature field depends on the choice of signature algorithm, as shown in Table 3-1. Encryption techniques, such as the Data Encryption Standard (DES) and RSA, shall not be used in indicia.

**Table 3-1. Indicium Data Elements**

| Data Elements | Barcode Data | Human-Readable Data | Length (bytes) | Field Number |
|---|---|---|---|---|
| **Indicia Version Number** | Yes | No | 1 | 1 |
| **Algorithm ID** | Yes | No | 1 | 2 |
| **Certificate Serial Number** | Yes | No | 4 | 3 |
| **Device ID** | | | | |
| - PSD Manufacturer ID | Yes | Yes | 2 | 4 |
| - PSD Model ID | Yes | Yes | 2 | 5 |
| - PSD Serial Number | Yes | Yes | 4 | 6 |
| **Ascending Register** | Yes | No | 5 | 7 |
| **Postage** | Yes | Yes | 4 | 8 |
| **Date of Mailing** | Yes | Yes | 4 | 9 |
| **Originating Address:** | | | | |
| - City, State, ZIP Code | No | Yes | — | — |
| - Registration ZIP Code | Yes | No | 4 | 10 |
| **Destination Delivery Point** | Yes | No | 5 | 11 |
| **Software ID** | Yes | No | 2 | 12 |
| **Descending Register** | Yes | No | 4 | 13 |
| **Mail Class or Category** | | | | |
| - Rate Category | Yes | No | 4 | 14 |
| - Endorsement (Mail Class) | No | Yes | — | — |
| **Digital Signature** | Yes | No | DSA 40 / RSA 128 / ECDSA 40 | 15 |
| **Reserved Field** | Yes | No | Variable Size | 16 |

The data elements listed in Table 3-1 shall be included in the indicium. The format of each human-readable data element shall be as specified in the DMM. These required elements are as follows:

- **Indicia Version Number.** This data element represents the version number assigned by the USPS to this indicia data set. It shall be represented by a 1-byte binary value.
- **Algorithm ID.** This data element identifies the digital signature algorithm used to create the digital signature in the indicium. It shall be represented by a 1-byte binary value.
- **Certificate Serial Number.** This data element represents the unique serial number of the PSD certificate issued by the IBIP Certificate Authority. It shall be represented by a 4-byte binary value.
- **Device ID: PSD Manufacturer ID.** This field represents the USPS-assigned 2-character ID for each Provider. The data shall be ASCII text.
- **Device ID: PSD Model ID.** This field represents the Provider's 2-character assigned model number for this PSD. This model number is furnished by the Provider and approved by the USPS. The data shall be ASCII text with the first character being numeric (0 – 9) and the second alpha (A – Z).

- **Device ID: PSD Serial Number**. This field represents the serial number assigned by the Provider to the given PSD. The data shall be represented by a 4-byte binary value.
- **Ascending Register**. This data element represents the total monetary value of all indicia ever produced during the life cycle of the PSD. The data shall be represented in a 5-byte binary value.
- **Postage**. This data element represents the amount of postage applied to this specific mailpiece. Postage applied is in accordance with the then-current USPS postage rates in the DMM or the IMM. The postage amount shall be represented in a 4-byte binary value in the numeric format 999.999. This field size supports the maximum amount of postage due on a single piece of mail in any mail class supported by the system.
- **Date of Mailing**. This data element represents the date of mailing for a mailpiece. The date of mailing shall be represented in a 4-byte binary value and has the numeric format YYYYMMDD in the barcode. The format of the date in the human-readable portion of the indicium is at the discretion of the Provider, except for the year, which shall be represented by 4 digits.
- **Originating Address: City, State, ZIP Code**. This human-readable field represents the city, state, and 5-digit ZIP Code for the registration post office. The indicium may display the ZIP Code rather than the city/state designation. In this case, the words "Mailed From ZIP Code" and the registration post office ZIP Code must appear in place of the city designation and state, respectively.
- **Originating Address: Registration ZIP Code**. This data element represents the registration post office delivery point identification. The format shall be a 5-digit numeric value represented by a 4-byte binary value in the indicium.
- **Destination Delivery Point**. This data element represents the destination delivery point. The format shall be a 5-byte binary value in the indicium. For domestic mail, the destination ZIP Code shall be used for this data element. For mail with an international destination, the first 2 bytes of this data element are the 2-character country code, per ISO 3166-1 Alpha-2 code, of the destination country. The next 2 bytes of the data element shall contain the 16-bit little endian value of the total number of characters in the address block. The last byte shall contain a binary zero.
- **Software ID**. This data element represents the client system software identification number, which has a length of no more than 3 digits. It shall be represented by a 2-byte binary value in the indicium.
- **Descending Register**. This data element represents the postage value remaining on the PSD. It shall be represented as a 4-byte binary value.
- **Rate Category.** This data element represents the postage class and rate. The USPS provides values for this field. This shall be a 4-byte alphanumeric ASCII value.
- **Digital Signature**. This data element represents the digital signature. The size of this data element is a function of the digital signature algorithm. If additional algorithms beyond those shown in Table 3-1 are approved for use by USPS the length of this field will be appropriately specified for those algorithms.

- **Reserved Field**. This field is included to allow for the future addition of data to the indicium. The field size shall be variable based upon the data content. The field shall have a binary value of zero.

The data that comprises the indicium must be input from either the PSD, the client system, or the user. The Provider shall obtain the specific values for the indicia version number, algorithm ID, and software ID fields from the USPS. The registration ZIP Code shall be assigned as part of the USPS user registration process.

### 3.2. Special Purpose Indicia

In addition to the standard mailpiece indicium discussed in 3.1, two additional indicia—Redate and Postage Correction indicia—may be required to address special cases. The requirements for these special purpose indicia are specified in 3.2.1 and 3.2.2.

### 3.2.1. Redate Indicium

A complete and accurate date shall be printed on the mailpiece. The complete date shall include the year, month, and day. The date of the indicium shall represent the actual date of deposit of the mailpiece. However, mail deposited after the day's last scheduled collection may bear the next scheduled collection date. In some cases, a correction of the date may be needed. In order to correct the date, the following data shall be included, in human-readable format only, on the mailpiece: the corrected date and the word "REDATE." The complete date shall include the month, day, and year, with the year being represented as 4 digits. There is no barcode in the redate indicium. The location of the redate indicium is specified in the DMM.

### 3.2.2. Postage Correction Indicium

The correct postage value shall be included in both the human-readable and barcode portions of the mailpiece indicium. If additional postage is to be added, a postage correction indicium can be placed on the mailpiece. The postage correction indicium shall contain both barcode and human-readable information. The data elements shall be as specified in Table 3-2, with the addition of the word "CORRECTION" to the human readable information The location of the postage correction indicium on the mailpiece is specified in the DMM.

**Table 3-2. Correction Indicium Data Elements**

| Data Elements | Barcode Data | Human-Readable Data | Length (bytes) | | | Field Number |
|---|---|---|---|---|---|---|
| **Indicia Version Number** | Yes | No | 1 | | | 1 |
| **Algorithm ID** | Yes | No | 1 | | | 2 |
| **Certificate Serial Number** | Yes | No | 4 | | | 3 |
| **Device ID** | | | | | | |
| - PSD Manufacturer ID | Yes | Yes | 2 | | | 4 |
| - PSD Model ID | Yes | Yes | 2 | | | 5 |
| - PSD Serial Number | Yes | Yes | 4 | | | 6 |
| **Ascending Register** | Yes | No | 5 | | | 7 |
| **Postage** | Yes | Yes | 4 | | | 8 |
| **Date of Mailing** | Yes | Yes | 4 | | | 9 |
| **Originating Address:** | | | | | | |
| - City, State, ZIP Code | No | Yes | — | | | — |
| - Registration ZIP Code | Yes | No | 4 | | | 10 |
| **Reserved Field 1** | Yes | No | 5 | | | 11 |
| **Software ID** | Yes | No | 6 | | | 12 |
| **Descending Register** | Yes | No | 4 | | | 13 |
| **Mail Class or Category** | | | | | | |
| - Rate Category | Yes | No | 4 | | | 14 |
| - Endorsement (Mail Class) | No | Yes | — | | | — |
| **Digital Signature** | Yes | No | DSA 40 | RSA 128 | ECDSA 40 | 15 |
| **Reserved Field 2** | Yes | No | Variable Size | | | 16 |

The first reserved field in the correction indicium replaces the Destination Delivery Point field in the standard indicium, and is the same length. This field shall have a binary value of zero.

### 3.3. Digital Signature Requirements

The digital signature required for the indicium is specified in this section. A digital signature shall be created by the PSD for each indicium and shall be placed in the digital signature field of the barcode. Multiple digital signature algorithms are supported by the IBIP. A Provider is at liberty to choose the digital signature algorithm most appropriate for its product. As of the date of these performance criteria, the IBIP supports the following algorithms:

- Digital Signature Algorithm (DSA)
- Rivest Shamir Adleman (RSA) Algorithm
- Elliptic Curve Digital Signature Algorithm (ECDSA)

If other digital signature algorithms are proposed, they will be considered by the USPS in accordance with the requirements in 3.3.4. It shall be the responsibility of the Provider to obtain from third parties any required rights, such as licenses, to use the approach chosen.

### 3.3.1. DSA Approach

One approach to providing the digital signature is the Digital Signature Standard (DSS), which incorporates the DSA algorithm, as specified in FIPS PUB 186-2, *Digital Signature Standard.* For a detailed discussion of the DSA signature creation and verification processes, see Chapter 4, Postal Security Device Performance Criteria.

### 3.3.2. RSA Approach

Another method for digital signature generation is by means of an algorithm known as the RSA algorithm, in accordance with "PKCS #1: RSA Encryption Standard," version 1.5, December 1, 1993. For a detailed discussion of the RSA signature creation and verification processes, see Chapter 4, Postal Security Device (PSD) Performance Criteria.

### 3.3.3. ECDSA Approach

Another approach to providing the signature functionality is to use the ECDSA, as specified in ANSI X9.62 Standard, Elliptic Curve Digital Signature Algorithm. For a detailed discussion of the ECDSA signature creation and verification processes, see Chapter 4, Postal Security Device (PSD) Performance Criteria.

### 3.3.4. Other Digital Signature Methods

Cryptographic, public-key signature methods, other than those addressed in these performance criteria, will be considered by the USPS if all the following conditions are met:

- The proposed method is shown to have a cryptographic strength equal to or greater than approaches delineated in these performance criteria.
- The proposed method can be supported by the planned USPS infrastructure with minimal or no increase in cost.
- The proposed method meets industry standards.

## 3.4. Indicia Design

This section addresses the requirements for the composition, position, printing resolution, error detection and correction, design layout, and reflectance standards for the indicium.

### 3.4.1. Indicium Composition

The following requirements address design-related issues concerning the composition of the indicium:

The indicium shall consist of both human-readable information and barcoded information in accordance with the requirements specified in 3.1.

- The human-readable information shall consist of, at a minimum, the Device ID (comprising the PSD Manufacture ID, PSD Model ID, and PSD Serial Number); the amount of the applied postage; the date of mailing; and the city, state, and 5-digit ZIP Code of the registration post office, as well as the endorsement (mail class). The indicium may display the ZIP Code rather than the city/state designation. In this case, the words "Mailed From ZIP Code" and the mailer's

delivery address ZIP Code must appear in place of the city designation and state, respectively.

- The human-readable portion of the indicium shall be in accordance with the DMM.
- The barcode region of the indicium shall be in accordance with the USPS-approved symbology.

### 3.4.2. Indicium Position

The requirements for positioning the indicium on the mailpiece are as follows:

- The indicium shall be printed or applied on the upper-right corner of the mailpiece, address label, or tag. It shall have a minimum distance of 1/4 inch from the right edge of the mailpiece and 1/4 inch from the top edge of the mailpiece. The barcode portion of the indicium shall be horizontally oriented.
- The positioning of the indicium shall not infringe on the areas allocated for the FIM or optical character reader (OCR) processing. As a reference, the general guidelines defining the dimensions for the FIM clear zones are detailed in DMM C100.5.2 and Publication 25, Designing Letter Mail. General guidelines defining the dimensions for the OCR read area are contained in DMM C830.

If a FIM is printed with the indicium for First-Class Mail, the requirements for FIM type and placement must be in accordance with the DMM.

### 3.4.3. Indicium Printing

As a general guideline, the barcode portion of the indicium should be printed using 300 dots per inch ("dpi); however, indicium readability is the ultimate determining factor of whether or not the system is usable for printing postage. Readability requirements may require more that 300 dpi and, under certain circumstances might be achieved with fewer than 300 dpi. Readability of the barcode portion of the indicium must assure a minimum USPS acceptance rate of 99.5%. For PDF417, a minimum 15-mil feature size shall be used for the "x" dimension. No dimension of the barcode portion of the indicium shall exceed 4 inches.

### 3.4.4. Error Detection and Correction

By adding error correction code words to the data message, the PDF417 symbology supports the detection and correction of lost or missing data. This symbology provides selectable levels of error protection by adding from 2 to 512 error correction code words. The error correction level shall be chosen to achieve a minimum USPS acceptance rate of 99.5%. The error correction code word level shall be a minimum of Level 4 as specified in the "Uniform Symbology Specification PDF417," July 1994. A higher error correction level shall be selected if needed to achieve the required USPS acceptance rate. If a USPS-approved symbology other than PDF417 is chosen, an equivalent level of error correction shall be applied by the chosen symbology.

### 3.4.5. Indicium Design Layout

The specific design layout of the indicium is at the discretion of the Provider. However, the indicium design shall conform to the guidelines as contained in the DMM. All indicia used in an IBI product must be preapproved by the manager of Postage Technology Management. This approval includes all elements in the indicium as defined by these performance criteria and includes the entire area within the following boundaries:

- The right-hand edge of the envelope.
- The top edge of the envelope.
- The bottom edge of the 2-D barcode or any other indicium element.
- The left-most edge of the 2-D barcode or any other indicium element.
- A 1/2 inch clear zone to the left of and below these indicium boundaries.

An approved indicium must not include any image or text within the boundaries defined above that is not required by the IBI performance criteria or is not a postal marking required or recommended by postal regulation.

### 3.4.6. Reflectance Standards

The requirements for the minimal standards for achieving acceptable reflectance measurements concerning the indicium and the background material shall be as specified in the "Uniform Symbology Specification PDF417," July 1994. If a symbology other than PDF417 is chosen, the requirements for the minimal standards for achieving acceptable reflectance measurements and the background material shall be as specified in the Uniform Symbology Specification of the chosen symbology. In addition, the mailpiece is required to meet USPS reflectance standards as specified in DMM C840.5.

# 4. POSTAL SECURITY DEVICE (PSD) PERFORMANCE CRITERIA

The Postal Security Device (PSD) provides security-critical functions for IBIP. The PSD shall be a hardware component and, when "married" with a specific user's register values constitutes a unique security device. The PSD shall have no functions except those described in these performance criteria.

The PSD core security functions are PSD initialization, cryptographic digital signature generation and verification, and secure management of the registers that track the remaining amount of money available for indicium creation (descending register) and the total postage value used during the life cycle of the PSD (ascending register). To ensure the security of IBIP processes, these core security functions, which are further described in 4.1.1, must be performed by the PSD. In order to perform these functions securely, the PSD shall be a tamper-resistant device that shall contain an internal random number generator, various storage registers, a date/time clock, and other circuits necessary to perform these functions. See 4.4 for details. The PSD shall comply with FIPS 140-2, *Security Requirements for Cryptographic Modules,* as described in 4.4.9. Compliance shall be validated through the National Institute of Standards and Technology (NIST) Computer Systems Laboratory's Cryptographic Module Validation Program. Additionally, the PSD shall comply with USPS criteria as detailed in this document. Where there are conflicts between FIPS standards and USPS criteria, the USPS criteria take precedence.

The PSD core security functions shall support implementation of the IBIP device authorization, finance, indicium creation, and device audit functions, which are further described in 4.3. Figure 4-1 illustrates the role the PSD plays in the creation of indicia.

## 4.1. PSD Interfaces

*TO BE SUPPLIED*

### 4.1.1. Certificate Authority

*TO BE SUPPLIED*

### 4.1.2. USPS Treasury

*TO BE SUPPLIED*

### 4.1.3. USPS

*TO BE SUPPLIED*

### 4.1.4. User (Customer)

*TO BE SUPPLIED*

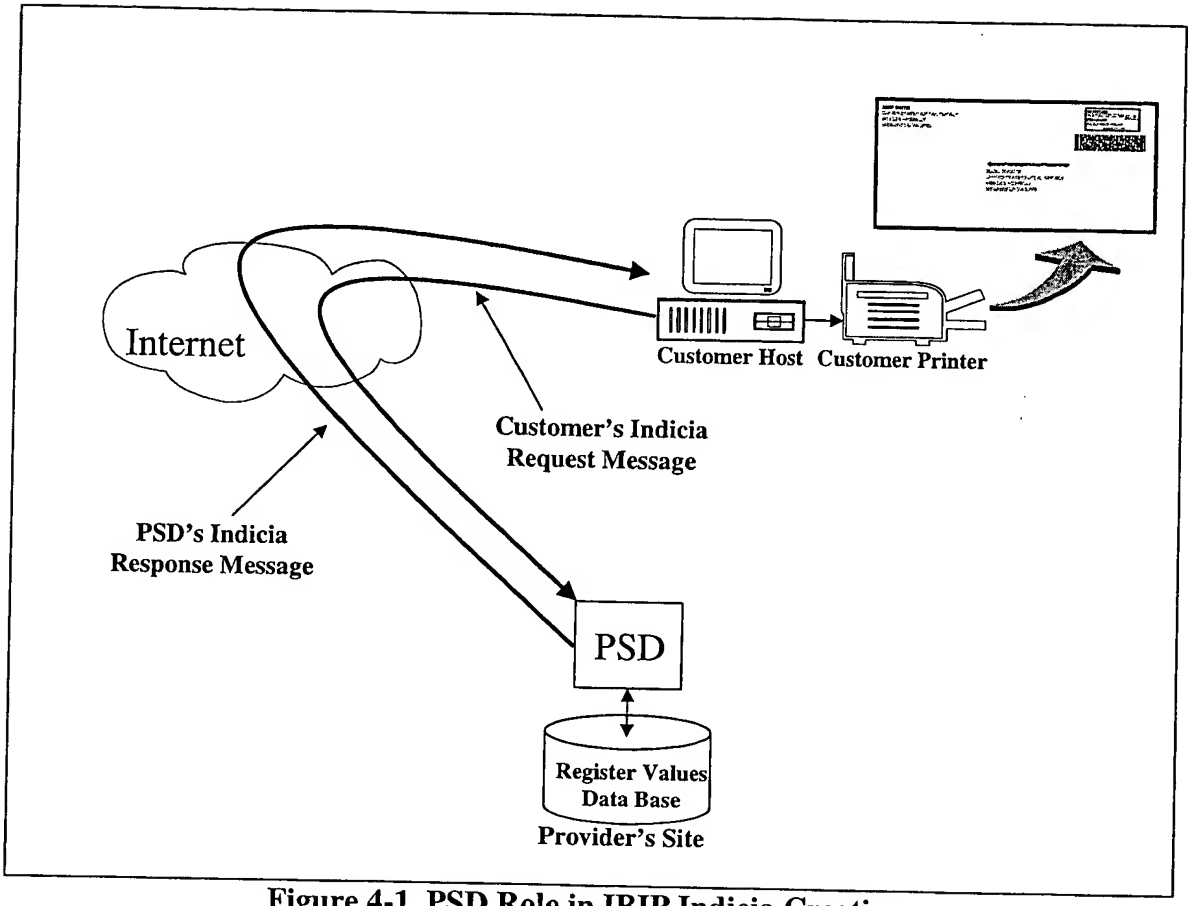



**Figure 4-1. PSD Role in IBIP Indicia Creation**

## 4.2. PSD Functional Requirements

Functional requirements for the PSD are specified in this section, with 4.2.1 through 4.2.3 specifying the PSD initialization function, reinitialization function, and PSD digital signature functions, respectively.

### 4.2.1. PSD Initialization

The PSD initialization function is the process used to load device-specific information for a given PSD. The process includes loading the device serial number and initializing the ascending and descending registers. In order to initialize the PSD, the Provider must load device-specific information that shall not change over the life cycle of the device (i.e., the period for which the device is associated to a specific user). The Provider shall assign a unique 4-byte PSD serial number to each PSD. During the initialization process, all internal registers and counters in the PSD shall be explicitly initialized to their intended initial values. When the PSD is initialized the value of the ascending register shall be set to US $000,000,000.000; and the value of the descending register shall be set to US $000,000.000.

### 4.2.2. PSD Reinitialization

A PSD may be reinitialized if the serial number of the device is changed and the ascending and descending registers are reset to zero. Reinitialization, with its assignment

of a new serial number, ends the life cycle of the device with the previous serial number. The Provider may reinitialize a PSD only when it is assigned to a new user. Reinitialization of the PSD is accomplished by assigning a new serial number to the PSD and resetting the ascending and descending registers to zero. When the new serial number is assigned to the PSD, the ascending register showing total postage used shall be reinitialized, and the old serial number for the PSD shall be reported to the USPS as a scrapped device.

### 4.2.3. PSD Digital Signature Functions

The PSD digital signature function uses the signing key generated for the PSD. This function shall provide data integrity and non-repudiation security services for IBIP indicia. Several alternatives for the digital signature function are identified in these performance criteria. Each of these alternatives implements a public-key cryptographic algorithm for the digital signature function. Providers may choose to implement one of the defined alternatives or may propose additional alternatives for consideration by the USPS.

The PSD shall implement DSA, RSA, or ECDSA, or another Provider-suggested and USPS-approved method for the generation and verification of digital signatures for the creation of indicia. The digital signature methodology used shall provide data integrity and non-repudiation services. If DSA, RSA, or ECDSA is used, the PSD must adhere to the requirements specified in 4.2.3.1 for DSA, 4.2.3.2 for RSA, or 4.2.3.3 for ECDSA, as well as the appropriate government and/or commercial standards. Requirements for other approved digital signature methods, if any, will be documented in future versions of this document.

#### **4.2.3.1.** DSA Requirements

A PSD must adhere to the requirements addressed in this section only if it implements the DSA signature method for IBIP. Wherever there are conflicts, the requirements in this section take precedence over those in the referenced published standards. If the Provider chooses to use DSA, the PSD shall implement the DSA as specified in FIPS PUB 186-2, *Digital Signature Standard*, to provide digital signature generation and verification functions. The PSD shall use the standard DSA parameters that are defined in FIPS PUB 186-2. Figure 4-2 illustrates the generic DSA signature generation and verification processes.

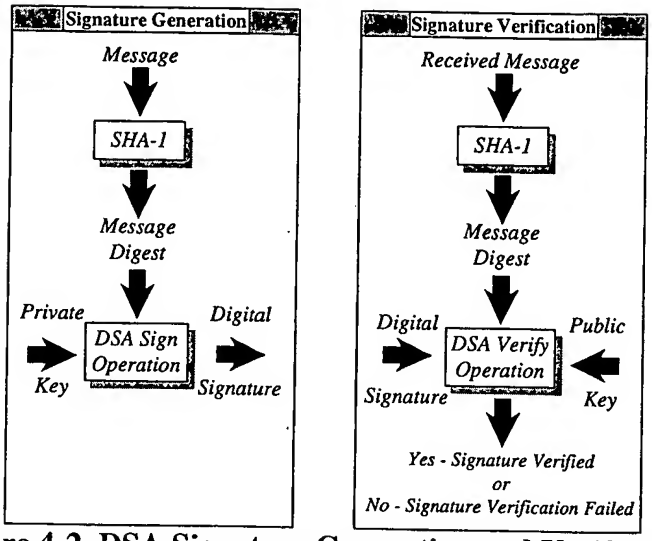



**Figure 4-2. DSA Signature Generation and Verification**

Using the default standard parameters specified in FIPS PUB 186-2, the PSD shall obtain or generate, as appropriate, the DSA parameters listed in Table 4-1 for signature generation, and in Table 4-2 for signature verification.

**Table 4-1. DSA Parameters for Signature Generation**

| Parameter | Source | PSD Storage | Comments |
|---|---|---|---|
| *p* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | DSA standard parameter common for all PSDs |
| *q* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | DSA standard parameter common for all PSDs |
| *g* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | DSA standard parameter common for all PSDs |
| *x* | Generated by the PSD during device authorization | Stored in nonvolatile memory until replaced or erased | PSD private key |
| *y* | Calculated by the PSD and output to client system during device authorization | Stored in the PSD IBIP certificate | PSD public key |
| *M* | Message created by the PSD based on client system inputs and internal register contents | Stored in the PSD only for the duration of DSA signature generation | Output to client system by the PSD |
| *k* | Generated by the PSD | Used for a single signature; erased after use | A new random value must be generated for each digital signature |
| *r* | Calculated by the PSD during the DSA sign operation | Result of DSA signature generation; erased after use | Output to client system by the PSD |
| *s* | Calculated by the PSD during the DSA sign operation | Result of DSA signature generation; erased after use | Output to client system by the PSD |

**Table 4-2. DSA Parameters for Signature Verification**

| Parameter | Source | PSD Storage | Comments |
|---|---|---|---|
| $p$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | DSA standard parameter common for all PSDs; same as parameter $p$ in Table 4-1 |
| $q$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | DSA standard parameter common for all PSDs; same as parameter $q$ in Table 4-1 |
| $g$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | DSA standard parameter common for all PSDs; same as parameter $g$ in Table 4-1 |
| $y$ | Loaded into the PSD from the client system | Stored in nonvolatile memory until replaced or erased | Public key of message originator |
| $M'$ | Message as received from message originator | Stored in PSD only for duration of DSA signature verification | Input from the client system to the PSD |
| $r'$ | Received from message originator | Stored in PSD only for duration of DSA signature verification | Input from the client system to the PSD |
| $s'$ | Received from message originator | Stored in PSD only for duration of DSA signature verification | Input from the client system to the PSD |
| $w$, $u_1$, $u_2$, $v$ | Generated by the PSD during signature verification process | Stored in PSD only for duration of DSA signature verification | The signature is verified if $v = r'$<br>PSD actions upon verification (or failure of verification) are specified in 3.2 |

If the DSA is used, the PSD shall create the digital signature using the standard DSA parameters as specified in the Digital Signature Standard in FIPS PUB 186-2. In accordance with that standard, the Secure Hash Algorithm (SHA-1), as specified in FIPS PUB 180-1, *Secure Hash Standard*, shall be used to create a 160-bit message digest. This is used in conjunction with the private key as inputs to the DSA signing operation and results in the digital signature as output. The input message for the SHA-1 shall be formatted as shown in Table 4-3. Although SHA-1 requires input to be blocked as multiples of 64 bytes, any required message pad is added by the algorithm itself and must not be included in the input data.

**Table 4-3. SHA-1 Message Input Format**

| Field Number | Field Name | Number of Bytes | Order* |
|---|---|---|---|
| 1 | Indicia Version Number | 1 | N/A |
| 2 | Algorithm ID | 1 | N/A |
| 3 | Certificate Serial Number | 4 | Start with least significant byte |
| 4 | PSD Manufacturer ID | 2 | N/A (text field) |
| 5 | PSD Model Number | 2 | N/A (text field) |
| 6 | PSD Serial Number | 4 | Start with least significant byte |
| 7 | Ascending Register | 5 | Start with least significant byte |
| 8 | Postage | 3 | Start with least significant byte |
| 9 | Date of Mailing | 4 | Start with least significant byte |
| 10 | Registration ZIP Code | 4 | Start with least significant byte |
| 11 | Destination Delivery Point | 5 | Start with least significant byte |
| 12 | Software ID | 6 | Start with least significant byte |
| 13 | Descending Register | 4 | Start with least significant byte |
| 14 | Rate Category | 4 | N/A (text field) |

*All binary fields are little endian format with least significant byte first, most significant byte last.

The PSD shall perform the hash function using the SHA-1, as specified in the *Secure Hash Standard*, FIPS PUB 180-1. The result of that operation shall be a 160-bit message digest that the PSD shall use in the creation of the DSA digital signature. The DSA algorithm generates two parameter values resulting from the DSA signing operation, which are referred to as "*r*" and "*s*." Each parameter is 160 bits in length. These two values shall be placed into the digital signature field of the barcode as shown in Figure 4-3.

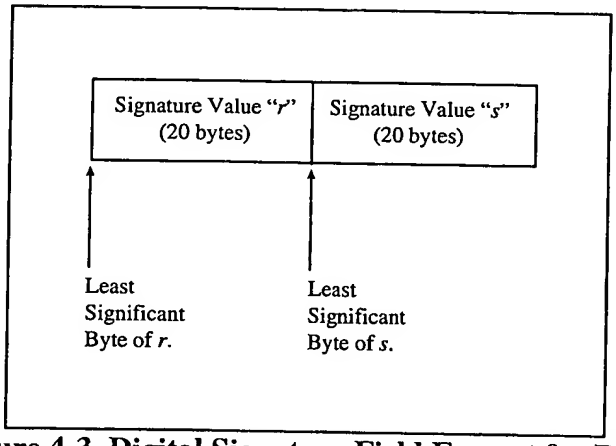



**Figure 4-3. Digital Signature Field Format for DSA**

**4.2.3.2.** RSA Requirements

A PSD must adhere to the requirements addressed in this section only if it implements the RSA signature method for IBIP. Wherever there are conflicts, the requirements in this section take precedence over those in the referenced published standards. If RSA is chosen, the PSD shall use RSA as specified in PKCS #1, Section 10, to implement digital signature generation and verification functions, using the standard RSA parameters as defined in "PKCS #1: RSA Encryption Standard," version 1.5, December 1993. Figure 4-4 illustrates the generic RSA signature generation and verification processes.

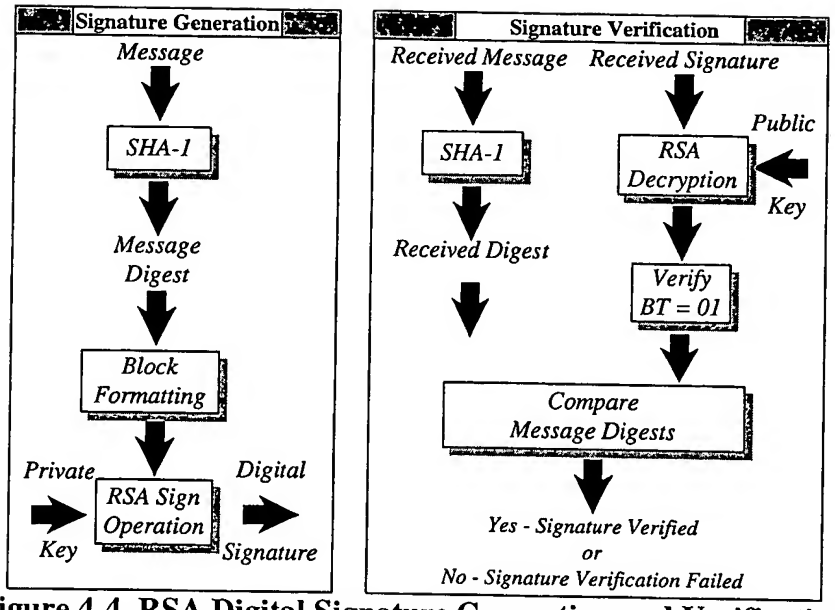



**Figure 4-4. RSA Digital Signature Generation and Verification**

The PSD shall create a digital signature by inputting the data to be signed to the SHA-1 and obtaining a message digest of 160 bits in length. Since the process of using the RSA algorithm to create a digital signature utilizes the SHA-1 hashing algorithm, as did DSA in the previous section, the input message for SHA-1 shall be the same as that illustrated in Table 4-3. However, in this case the 160-bit SHA-1 output shall be block formatted in accordance with the RSA Data Security Standard, PKCS #1, Section 8. Specifically, the SHA-1 output is placed in the data field (D) of the signature block (SB), as follows:

$$\mathbf{SB = 00 \parallel BT \parallel PS \parallel 00 \parallel D}$$

The block type (BT) shall be a single octet with the value of 01 indicating a private key operation. The padding string (PS) shall be 105 octets with each octet being set to the value FF. This then makes the length of the signature block equal to the length of the public-key modulus (1024 bits). This resulting block is then transformed using the private key, and the result is placed in the digital signature field of the indicium.

If RSA is used, the PSD shall generate the parameters listed in Table 4-4 for RSA signature generation and Table 4-5 for RSA signature verification.

**Table 4-4. RSA Parameters for Signature Generation**

| Parameter | Source | PSD Storage | Comments |
|---|---|---|---|
| *p* | Generated by the PSD during device authorization | N/A | Needed to calculate the PSD's modulus *n* |
| *q* | Generated by the PSD during device authorization | N/A | Needed to calculate the PSD's modulus *n* |
| *N* | Modulus for the PSD, calculated during authorization | Stored in nonvolatile memory until replaced or erased | $n = pq$, stored as part of the PSD's public key |
| *d* | Generated by the PSD during device authorization | Stored in nonvolatile memory until replaced or erased | PSD's private key |
| *e* | IBIP established parameter (shall be set = 65537) | Stored in nonvolatile memory until replaced or erased | RSA exponential value used in the signature verification process; part of PSD's public key |
| *S* | Generated during the RSA signature generation process | Stored in PSD only for duration of RSA signature generation | Result of the RSA signature generation that is output to the client system |

**Table 4-5. RSA Parameters for Signature Verification**

| Parameter | Source | PSD Storage | Comments |
|---|---|---|---|
| *n* | X.509 Certificate of the signer | Stored in nonvolatile memory until replaced or erased | Part of the signer's public key |
| *e* | IBIP established parameter (shall be set = 65537) | Stored in nonvolatile memory until replaced or erased | |
| *M* | Message generated by the sender | Stored in PSD only for duration of RSA signature verification | $n = pq$, stored as part of the PSD's public key |
| *S* | Generated by the message originator during message creation | Stored in PSD only for duration of RSA signature verification | Input from the client system to the PSD |
| *MD* | Message digest resulting from processing the signature of the message | Stored in PSD only for duration of RSA signature verification | |
| *MD'* | Generated using the received message during the RSA signature verification process | Stored in PSD only for duration of RSA signature verification | RSA signature is verified if $MD' = MD$ |

The PSD shall perform the hash function using the SHA-1 as specified in the Secure Hash Standard in FIPS PUB 180-1. The result of that operation shall be a 160-bit message digest that the PSD shall use in the creation of the RSA digital signature. If the RSA methodology is used, the signature block generated by application of the RSA is signed using the private key, and the result is placed into the digital signature field of the indicium.

**4.2.3.3.** Elliptic Curve Digital Signature Algorithm Requirements

A PSD must adhere to the requirements addressed in this section only if it implements ECDSA for IBIP. Wherever there are conflicts, the requirements in this section take precedence over those in the referenced published standards. If Elliptic Curve technology

is chosen, the PSD shall use the ECDSA algorithm as specified in the ANSI X9.62 Standard to implement digital signature generation and verification functions. Figure 4-5 illustrates the generic ECDSA signature generation and verification processes.

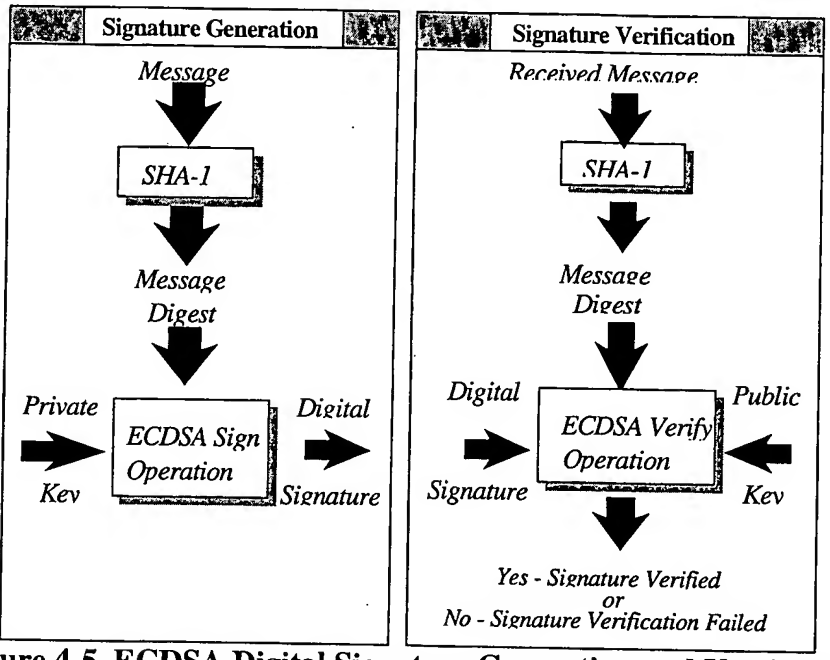



**Figure 4-5. ECDSA Digital Signature Generation and Verification**

If the ECDSA algorithm is used, the PSD shall generate or obtain, as appropriate, the parameters listed in Table 4-6 for ECDSA signature generation and Table 4-7 for ECDSA signature verification.

**Table 4-6. ECDSA Parameters for Signature Generation**

| Parameter | Source | PSD Storage | Comments |
|---|---|---|---|
| $q$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; defines the underlying finite field |
| $f$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; defines the basis for field representation |
| $a, b$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | Two ECDSA standard parameters common for all PSDs; defines the elliptic curve to be used |
| $P$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; defines a point of the curve of prime order |
| $n$ | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; the order of the point $P$; must be a prime which is greater than $2^{150}$ |

| | | | |
|---|---|---|---|
| *d* | Generated by the PSD during device authorization | Stored in nonvolatile memory until replaced or erased | PSD private key |
| *Q* | Calculated by the PSD and output to the client system during device authorization | Stored in the PSD IBIP certificate | PSD public key |
| *M* | Message created by the PSD based on client system input and internal register contents | Stored in the PSD only for the duration of the ECDSA signature generation calculation | Output to client system by the PSD |
| *k* | Generated by the PSD | Used for a single signature; erased after use | A new random value generated for each signing operation |
| *r, s* | Calculated by the PSD during the ECDSA sign operation | Result of ECDSA signature generation; erased after use | Output to client system by the PSD |

**Table 4-7. ECDSA Parameters for Signature Verification**

| Parameter | Source | PSD Storage | Comments |
|---|---|---|---|
| *q* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; defines the underlying finite field; same as parameter *q* in Table 4-6 |
| *f* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; defines the basis for field representation; same as parameter *f* in Table 4-6 |
| *a, b* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | Two ECDSA standard parameters common for all PSDs; defines the elliptic curve to be used; same as parameters *a* and *b* in Table 4-6 |
| *P* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; defines a point of the curve of prime order; same as parameter *P* in Table 4-6 |
| *n* | Loaded into the PSD during device initialization | Stored in nonvolatile memory until replaced or erased | ECDSA standard parameter common for all PSDs; the order of the point P; same as parameter *n* in Table 4-6 |
| *Q* | Loaded into the PSD from the client system | Stored in PSD only for duration of ECDSA signature verification | Public key of message originator |
| *M'* | Message as received from message originator | Stored in PSD only for duration of ECDSA signature verification | Input from the client system to the PSD |

| | | | |
|---|---|---|---|
| $r'$, $s'$ | $r$, $s$ values received from message originator | Stored in PSD only for duration of ECDSA signature verification | Input from the client system to the PSD |
| $w$, $u_1$, $u_2$, $v$ | Intermediate values generated by the PSD during signature verification | Stored in PSD only for duration of ECDSA signature verification | The signature is verified if $v = r'$ |

The PSD shall perform the hash function using the Secure Hash Algorithm (SHA-1), as specified in the *Secure Hash Standard*, FIPS PUB 180-1. The result of that operation shall be a 160-bit message digest that the PSD shall use in the creation of the ECDSA digital signature. Since the process of using the ECDSA algorithm to create a digital signature utilizes the SHA-1 hashing algorithm, as did DSA above, the input message for SHA-1 shall be the same as that illustrated in Table 4-3. This message digest and the private key are then input to the ECDSA signing operation and the resulting output is the digital signature.

The ECDSA algorithm generates two parameter values resulting from the ECDSA signing operation, which are referred to as "*r*" and "*s*." Each parameter is 160 bits in length. These two values shall be placed into the digital signature field of the barcode in the same manner as for DSA, as shown in Figure 4-3.

### 4.2.4. Register Management Functions

The intent of the register management function is to ensure the financial registers in the PSD (i.e., the ascending and descending registers) operate correctly and accurately reflect USPS revenue. Providers shall choose for this purpose technology that even a sophisticated, knowledgeable attacker could not defeat so as to alter the register values or successfully defraud the USPS. The PSD shall store and manage ascending and descending registers in nonvolatile memory to support the IBIP finance and indicia creation functions as discussed in 4.3. The management of these registers is specified in this section.

Each register shall represent a monetary value. The monetary values shall be measured in 1/10 of 1-cent increments. The ascending register shall consist of 5 bytes of binary data. The descending register shall consist of 4 bytes of binary data. Therefore, the register values shall be interpreted as follows:

- Ascending Register: US $999,999,999.999
- Descending Register: US $999,999.999

Subject to the requirements of this section, the ascending register shall support any postage usage value less than US $1 billion; the descending register shall support any postage value less than US $1 million. The PSD shall be designed such that neither the ascending register nor the descending register shall ever exceed the maximum allowable value. In the event that the ascending register reaches its maximum value, further indicia

creation operations shall be disabled. The sum of the ascending and descending registers shall not be able to exceed US $1 billion.

When the PSD receives valid notification of the funds on deposit with the USPS Treasury (or an update thereof) for a specific user through the Financial Institution interface, the user's descending register value shall be increased by the amount specified in the notification.

When the user's client system requests the creation of an indicium, the PSD shall perform several operations using the ascending and descending registers. First, the PSD shall compare the requested postage amount input from the user's system with the allowable limits currently in effect for the PSD for printing postage. If the requested postage amount is greater than or equal to the minimum limit and less than or equal to the maximum limit, the PSD shall proceed with its register management functions. If the requested postage amount is not within the allowable limits, an appropriate error message shall be returned to the user. The allowable requested postage amount shall be compared to the value contained in the descending register. When the descending register contains sufficient value, the register values shall change in accordance with Table 4-8. If an insufficient value remains in the descending register, the PSD shall return an appropriate message to the user and abort the indicium creation function.

**Table 4-8. Ascending and Descending Register Operations**

| IBIP Function | Ascending Register Operation | Descending Register Operation |
|---|---|---|
| Indicium Creation | The value contained in the ascending register shall increase by the postage amount specified by the client system | The value contained in the descending register shall decrease by the postage amount specified by the user's client system |
| Finance (Upon notification of funds on deposit with USPS Treasury) | The value contained in the ascending register shall be unchanged by the finance function | The value contained in the descending register shall increase by the amount of postage value contained in a valid funds notification |

After completion of PSD initialization, the PSD shall have no mechanism available to alter the value contained in either the ascending register or the descending register except as specified above. Upon request of the user, the current values of the ascending and descending registers shall be output to the user's client system for display to the user. This function allows the user to determine the remaining postage value contained in the PSD and the total amount of postage applied by that PSD.

## 4.3. PSD Requirements to Implement IBIP Functions

This section presents the requirements for the proper implementation of IBIP functions. The three IBIP functions (device authorization, finance, and indicium creation), in conjunction with the PSD initialization function, ensure that only authorized PSDs support the creation of valid indicia on mailpieces. Additionally, these functions provide the means to detect illicit use of a PSD.

### 4.3.1. IBIP Device Authorization

The IBIP authorization process ensures that only an authorized device can support the creation of a valid indicium. The Provider shall authorize a PSD for use by a specific registered user. Once a PSD is authorized, the finance functions must be performed before the first indicium is created. The authorization of a PSD is the process used to load user-specific information into the PSD. It includes generating all cryptographic keys, loading certificates, and loading the manufacture identification number and model identification number components of the device identity. During the IBIP device authorization process, the Provider shall tailor the PSD for a particular user and fully enable it to perform IBIP functions. Prior to performing the device authorization functions, the PSD must have been initialized or reinitialized in accordance with 4.2.1.

A Provider may reprogram a PSD with new device authorization information if there are changes to relevant user authorization information, such as a change to the registration ZIP Code. The Provider must reprogram a PSD with the appropriate device authorization information if the Provider issues the PSD to a different user or if there is an upgrade to the PSD. When user authorization information changes, the Provider must interface with the USPS infrastructure to ensure user information is updated as required. Device authorization does not include resetting the value in the ascending or descending register. These values can be set only when the device is initialized or reinitialized.

PSD device authorization shall include the following steps:

- Load Device ID Elements. During device authorization, each PSD shall be loaded with the 2-character manufacturer ID and a 2-character model identification. The USPS will assign the manufacturer ID. The USPS will assign the model numbers based on recommendations made by the Provider. The model number is 2 characters with the first character being numeric, and the second character being alpha.
- Load User Authorization Information. During device authorization, each PSD shall be loaded with user-specific information including the registration ZIP Code.
- Private/Public Key Processing. The PSD shall handle public and private key processing as detailed in Table 4-9. The Provider shall be responsible for passing the public key to the IBIP certificate authority and obtaining the certificate containing the PSD's public key.
- Load Maximum/Minimum Postage Amount. The PSD shall be loaded with the maximum and minimum postage values that the PSD is allowed to process. The Provider determines the minimum value. The maximum value is in accordance with 3.1.The PSD shall have a mechanism to update the range of minimum and maximum allowable postage when the USPS changes applicable regulations.
- PSD Upgrades. Any revisions to the PSD, including software upgrades to existing PSDs, shall result in a new 2-character model number, making it necessary to reauthorize the device by loading the new model identification number into the PSD. However, at no time shall any revisions to the PSD result in changing the PSD's register values or serial number, unless the PSD is reinitialized. Any

revision to the PSD, including software upgrades of existing PSDs, must be approved by the USPS. The USPS must also approve the process for implementing the upgrade.

### 4.3.2. IBIP Finance Function

The fundamental role of the PSD in the implementation of the IBIP finance function is to request, accept, and process notification of the funds a user has made available with the USPS Treasury. This is accomplished through the Financial Institution Interface. When valid notification is received, the IBIP finance function shall load postage value into the PSD. In addition, the IBIP finance function allows the user to obtain a refund of all postage remaining when the PSD is withdrawn from service.

To support IBIP finance functions, all communications between the user and the Provider infrastructure must authenticate the sender and verify the message. The specific authentication/verification methods for these transactions are Provider-specific and are beyond the scope of this document. The authentication methods may vary from Provider to Provider, but they must be approved by the USPS.

**Table 4-9. Private/Public Key Processing**

| Step | DSA or ECDSA | RSA |
|---|---|---|
| 1 | PSD shall internally generate the private key | PSD shall internally generate the public key |
| 2 | PSD shall calculate the public key | PSD shall calculate the private key |
| 3 | PSD shall store the private and public keys in nonvolatile memory | Same |
| 4 | PSD shall output the public key to the Provider | Same |
| 5 | PSD shall accept the certificate from the Provider | Same |
| 6 | PSD shall compare the stored public key with the received certificate's public key | Same |
| 7 | If the comparison in step 6 fails, go to step 1 | Same |
| 8 | If the comparison in step 6 is successful, store the number of the certificate | Same |

### 4.3.3. Indicium Creation Function

The role of the PSD in the indicium creation function is to perform security-critical processes as described in this section. It is the responsibility of the user's client system to use the information provided by the PSD to create the indicium. Upon failure of any of the processes described in this section, the PSD shall issue an appropriate error message to the client system. The PSD and the user's client system shall jointly perform functions necessary to create a valid indicium in accordance with the performance criteria for the indicium in Chapter 3. The PSD shall accept input from the user's client system and use data internal to the device itself to create signed data elements for selected fields in the indicium. When a user needs to add postage value to the PSD, the user will execute a funds transfer to the USPS.

#### 4.3.3.1. Indicium Creation User Client Request

The user's client will initiate the postage download process by creating an Indicia Request Message (IRM) and passing that IRM to the Provider's centralized PSD site. The Provider's centralized site must authenticate the sender and must verify the data

transmitted to detect data modification and replay. The format of this request is at the discretion of the PSD Provider; however, this IRM shall contain all of the information and data necessary for the customization of the mailpiece. At a minimum, this shall include a unique user ID, the amount of the postage, the date of mailing, the destination ZIP Code, the software ID, and the rate category. Whether an IRM is structured to allow a user to request more than one indicia at a time is left up to the Provider's ingenuity in developing an application-level protocol for the IRM. If such a "multiple IRM" were to be used, it shall be necessary to include the customization data for each requested indicia. It shall be the Provider's responsibility to determine the authentication and verification method and the data contained in this IRM; however, such methods and the message data must be approved by the USPS. It shall be the Provider's responsibility to ensure that all messages and transmissions are completed without error and that any erroneous messages are trapped and handled properly.

**4.3.3.2.** Indicium Creation PSD Response

The Provider's centralized PSD site, upon receipt of a user IRM, would then perform the necessary checks to ensure that the user has the required amount of money on deposit with the USPS. If so, the PSD shall respond with a PSD Response Message (PSDRM), which would contain a digitally signed indicia for each mailpiece requested in the user's IRM. The signed data in the PSDRM would, at a minimum, include the unique user ID, the user's ascending register, the postage amount, the date of mailing, the user registration ZIP Code, the destination ZIP Code, the software ID, the user's descending register, and the rate category. This user interaction with the PSD is illustrated in Figure 4-1.

**4.3.3.3.** Indicia Request Message Security Requirements

Data integrity requirements for the interaction depicted in Figure 4-1 consist of the following:[1]

- The IRM shall be digitally signed by the user using a USPS-approved "Public-Key" algorithm (sometimes referred to as an asymmetric algorithm) with a private key unique to that user. This key shall hereinafter be denoted by $V_{CUST}$.
- The signature on the IRM, upon reception by the PSD, shall be verified using the corresponding public key of the user, $U_{CUST}$.
- The indicia signature shall be created using a USPS approved "Public-Key" algorithm with a private key unique to the PSD and denoted by $V_{PSD}$.
- The indicia signature shall be verified by the USPS mailpiece audit function using the PSD's corresponding public key, $U_{PSD}$.

[1] The remainder of this document uses the following notation for cryptographic keys: When referring to the keys associated with an asymmetric algorithm, the public key is denoted by $U_x$ while the corresponding private key is denoted by $V_x$, where the subscript is used to distinguish between different versions of the same type of key. When referring to a symmetric algorithm, the key is denoted by $K_x$, where again, the subscript is used for different versions.

**4.3.3.4.** PSD Response Message Security Requirements

Signed indicia data sent back from the PSD to the user in the PSDRM can potentially be electronically intercepted, printed, and used in unauthorized mailings. Of course, such duplicate indicia would be recognized as such during the mailpiece audit process (i.e., duplicate database search); however, the only "electronic tracks" available to an investigative body would lead back to the authorized user, not to the perpetrator. As a result, the confidentiality requirements for the interaction depicted in Figure 4-1 consist of either of the following:

- The PSDRM shall be encrypted prior to being sent to the user using a USPS approved "Public-Key" algorithm with a public key, $U_{PSDRM}$. Further, $U_{PSDRM}$ shall be the public portion of a key pair ($U_{PSDRM}$, $V_{PSDRM}$), where $V_{PSDRM}$ is unique to the user. Additionally, the PSDRM shall be decrypted upon reception by the user using $V_{PSDRM}$.
- The PSDRM shall be encrypted prior to being sent to the user using a USPS approved "Secret-Key" algorithm (sometimes referred to as a symmetric algorithm). Further, the key used by this "Secret-Key" algorithm, denoted by $K_{PSDRM}$, shall be unique between the user and server.

These confidentiality requirements are further illustrated in figure 4-6.

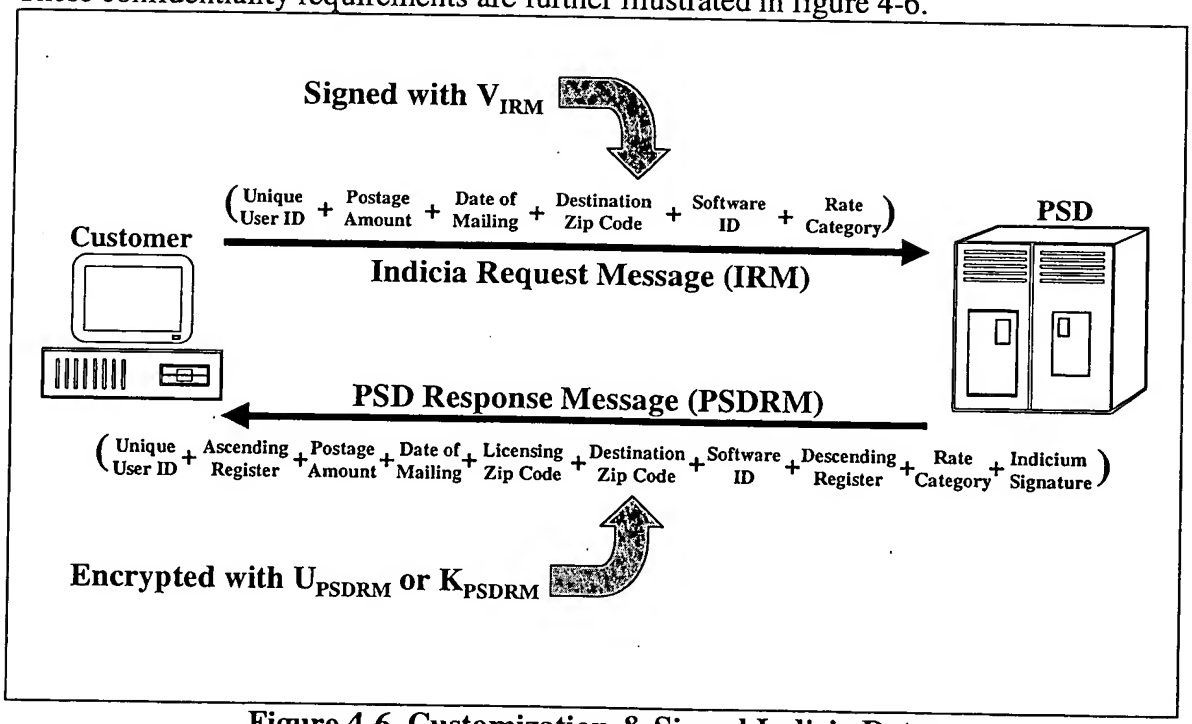



**Figure 4-6. Customization & Signed Indicia Data**

## 4.4. PSD Security

This section describes the security requirements to which the PSD shall conform. It is not the intent of these performance criteria to require a particular design. The requirements presented in this section are those necessary to ensure the integrity of the PSD and the IBIP system.

### 4.4.1. PSD Physical Security

The Cryptographic Subsystem of the PSD (CSPSD) shall be designed and implemented in accordance with FIPS PUB 140-2. The CSPSD shall conform to the FIPS requirements for overall security level 3 and physical security level 3, and as specified in Table 4-10. When there is a conflict between the FIPS requirements and the table, Table 4-10 takes precedence.

**Table 4-10. FIPS 140-2 CSPSD Requirements**

| FIPS 140-2 Design Category | Proposed CSPSD Performance Criteria/ FIPS 140-2 Requirements | Comment |
|---|---|---|
| Crypto Module | Documentation Required:<br>– CSPSD Description (by Provider)<br>– Specification of CSPSD cryptographic module and its cryptographic boundary (by Provider)<br>– CSPSD security policy (by Provider) | Provider CSPSD description and performance criteria must comply with these CSPSD performance criteria. Provider PSD security policy must comply with IBIP security policy. |
| Module Interfaces | Paths explicitly defined (by Provider):<br>– Power and control paths<br>– Input data<br>– Separate inputs for data and plaintext security parameters (keys and access control data), or single input if security parameters are protected<br>– Output data and status<br>– Optional: maintenance access (Provider proprietary) | Message and data formats must be approved by the USPS, as described in these performance criteria |
| Roles | Authorized roles:<br>– Crypto officer (Provider)<br>– Maintenance (Provider)<br>– Access control — authentication by role for user, Provider, individual (optional) | Minimum access control shall satisfy security level 3 (role-based) access; security levels 3 and 4 (individual) access is optional; at least a PIN/password entry is needed for access control for either case |
| Services | Initiate and run self-tests<br>Output module status<br>Output module alarms<br>CSPSD core and IBIP functions<br>No bypass capability | Self-tests — see below |
| Finite State Machine Model | Comply with FIPS PUB 140-2, section 4.4 design and documentation requirements | Required documentation from Provider/manufacturer |
| Physical Security | CSPSD Physical Security requirements | Security level 3 |
| Environmental Failure Protection or Testing (EFP/EFT) | Employ environmental failure protection features or undergo environmental failure protection testing for accreditation | Implemented to counter a potential tampering mode (especially voltage and temperature), Security level 4 |
| Software Security | Required documentation:<br>– Software design<br>– Relationship of design to security policy<br>– Annotated complete source code<br>– Implement in high-level language unless low-level language essential or high-level language not available | Additional documentation required from Provider/ manufacturer |

| FIPS 140-2 Design Category | Proposed CSPSD Performance Criteria/ FIPS 140-2 Requirements | Comment |
|---|---|---|
| Operating System Security | Not applicable | Required only if operator has means of loading device software |
| Key Management | Key generation: Only internal generation of CSPSD's public and private keys<br>Key distribution: PSD public key sent to CA upon generation for inclusion in certificate | No key extraction except PSD public key |
| Crypto Algorithms | Implement DSA, RSA, or ECDSA, or other USPS-approved signature generation and verification algorithm | Provider may need to obtain necessary rights to use |
| Electromagnetic Interference and Compatibility (EMI/EMC) | Comply with EMI/EMC requirements specified by FCC Part 15, Subpart J, Class B (i.e., for home use); conforms to security levels 3 and 4 | Primarily for compatibility with other electronic devices |
| Self-Tests | Statistical random number generator test performed during initialization and again at authorization.<br>Power-up self-tests:<br>– Crypto algorithm (known answer)<br>– Error detection code or authentication<br>– Critical functions<br>Conditional tests:<br>– TBD by Provider (pair-wise consistency, software/firmware load, manual key entry, continuous random number generator) | Testing must ensure proper operation of PSD functions |

### 4.4.2. PSD Contents

The CSPSD shall include a FIPS 140-2-compliant random number generator.

### 4.4.3. PSD Internal Storage

The CSPSD internal storage data requirements are as follows:

- IBIP common parameters.
- Any other authentication/verification data required for the Provider product that is common to all user records.

If the Revenue Sensitive Register Values (RSRVs) and their associated data elements are not stored within the cryptographic boundary of the PSD (see 4.4.5), then the storage of those values shall hereinafter be referred to as the PSD Repository. The PSD Repository shall store the following data elements for each user:

- User's Originating ZIP Code.
- User's Ascending register.
- User's Descending register.
- Maximum/minimum postage values for that user.
- User's PSD X.509 certificate serial number.
- Device ID (PSD manufacturer ID, PSD model ID, PSD serial number).
- PSD private key, $V_{PSD}$.

### 4.4.4. PSD Software

The CSPSD shall comply with the FIPS PUB 140-2 software security requirements appropriate for its security level. Additionally, if applicable, the CSPSD shall comply with the operating system requirements in accordance with FIPS PUB 140-2.

### 4.4.5. PSD Tamper Resistance

The CSPSD shall have an explicitly defined perimeter that establishes the physical bounds of the module. Included within this boundary shall be all cryptographic components, all processors, software, firmware, and other components that implement IBIP required CSPSD processes and functionality.

The CSPSD shall use tamper detection countermeasures that respond to tampering by disabling the CSPSD from further use until completion of a physical inspection by USPS. The CSPSD shall not provide any capability to bypass the security services of the cryptographic module. The physical security protections of the CSPSD must not be easily tampered, circumvented, or disabled.

### 4.4.6. PSD Access Control

The CSPSD shall employ security mechanisms to restrict unauthorized physical access to the contents of the module, thereby deterring unauthorized use and unauthorized modification. The CSPSD shall directly authenticate any person who is authorized to perform the role of operator of the CSPSD, for example, by using a password and PIN to meet FIPS PUB 140-2 (see Table 4-10).

### 4.4.7. PSD Key Handling

CSPSD key entry and output, distribution, and storage shall be in conformance with FIPS-approved methodologies and with the IBIP Key Infrastructure.

Within the CSPSD, keys may be stored in plaintext form in the cryptographic module and shall not be accessible from outside the device. Keys stored within the RSRV portion of the PSD shall be stored in encrypted form, and the key used to encrypt them shall itself be stored within the cryptographic boundary of the CSPSD. The PSD shall include a mechanism to ensure that stored keys shall remain associated with the correct device ID and the user to whom the key was issued. The CSPSD shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected security parameters within the module. There shall be no capability to zeroize the ascending or descending registers except during initialization or reinitialization.The PSD shall not output its private keys.

### 4.4.8. PSD Input and Output Requirements

The data ports for unencrypted, critical CSPSD-security parameters shall be physically separated from other data ports. If plaintext authentication data (e.g., password or PIN) are used, the entry port shall be physically separate from any other cryptographic module data entry port and allow for direct entry of the data. The CSPSD shall provide an output to indicate the status of the device.

### 4.4.9. FIPS 140-2 Compliance

The PSD shall be tested for conformance with FIPS PUB 140-2, physical security level 3, and FIPS PUB 140-2 EFP/EFT Requirements level 4. Testing shall be through the Cryptographic Module Validation Program by a cryptographic module testing laboratory that is a member of an accredited National Voluntary Laboratory Accreditation Program. When the PSD is shown to be in conformance with FIPS PUB 140-2 as required by these performance criteria, it shall receive a validation certificate. This testing shall include any attack procedures known to the USPS, whether or not such procedures are included in the current FIPS PUB 140-2 requirements. In addition, the PSD shall be evaluated and approved by the USPS and receive IBIP approval.

# 5. Centralized PSD Site Security

This chapter delineates the security requirements for the centralized PSD site.

## 5.2. PSD Repository Requirements

If the Revenue Sensitive Register Values (RSRVs) of the PSD are not stored within the cryptographic boundary of the PSD, that storage is referred to as the PSD Repository. If this PSD Repository exists, it is assumed that each record of this database will correspond to a specific user account where the data elements stored in that record are listed as in 4.4.3. To protect USPS revenue, the following security requirements shall apply to the PSD Repository and to the facility that houses that repository:

- Control for physical access to the facility that houses the PSD Repository.
- Encryption of the user's private key ($V_{PSD}$) and, at the discretion of the Provider, other data elements while resident in the repository. Further, the key used for this encryption function shall be resident in its usable form only within the protective confines of the CSPSD. A small cadre of essential personnel may have access to this key for backup or maintenance purposes but only in a dual-control fashion (i.e., split-knowledge components). Further, it is required to change this encryption key on a periodic basis or upon any essential personnel terminations.
- Record level cryptographic based data integrity techniques shall be in place for use and maintenance of the repository.

## 5.3. Cryptographic Requirements

When a user's record is retrieved by the CSPSD from the PSD Repository due to an attempt to satisfy an Indicia Request Message (IRM) or to update that record due to a change in one or more of the data elements (i.e., update of user funds on deposit, change in user's originating ZIP Code, etc.), that record shall be available only in its plaintext form within the cryptographic boundary of the CSPSD. In other words, the encrypted record is retrieved from the PSD Repository and then sent to the CSPSD, where it is decrypted. Following decryption, the integrity of the data record shall be verified before the data elements are used and subsequently updated. Once updated, the integrity value is recalculated and the updated record is then re-encrypted before being sent back to the PSD repository for storage.

If, upon decryption of the record, its integrity value cannot be verified, the Provider must have a recovery procedure in place in order to assure the protection of USPS revenue. It is the responsibility of the Provider to develop this recovery procedure (for example, multiple copies of the user's record in different locations). However, whatever methodology the Provider desires to implement is subject to USPS approval.

## 5.4. Availability Requirements

The Provider shall develop procedures for refunding any residual postage amounts in a given user's account if and when that user is denied legitimate use or access to the account.

### 5.5. Access Control Requirements

The Provider shall develop a strong access control methodology to ensure that only legitimate, authorized users can gain logical access to the centralized PSD site. In this same regard, the Provider shall develop a methodology to protect against replay of previous indicia request messages (IRMs). Without replay protection, the signed indicia request messages sent from the user to the server could be intercepted and replayed to the server at some later time. This might result in a user's funds being tapped to fraudulently pay for someone else's indicia. The provider shall develop an IRM replay protection mechanism, and after USPS approval of that mechanism, the Provider shall implement it.

### 5.6. PSD Back-up and Recovery

The Provider shall develop a back-up and recovery mechanism to ensure the protection and integrity of USPS revenue. The recovery mechanism must not compromise USPS revenue (i.e., generally recovery mechanisms are limited in the sense that they lose any updating that occurs between the last back up and the failure that precipitates the recovery). However, the Provider-developed back-up and recovery mechanism to be implemented here shall not suffer from this limitation. The methodology used by the Provider shall be subject to approval by the USPS.

### 5.7. Continuous Operations

Since the user has prepaid for postage, the user must be able to make use of that postage at any time. Therefore, the Provider's implementation must allow a user access under all possible circumstances. For example, a 24-hour, 7-day-a-week continuous operation with redundant sites and load leveling mechanisms to ensure that heavy usage volumes do not limit or restrict users may be a technique to satisfy this requirement. However, the methodology implemented by the Provider to satisfy this requirement is subject to approval by the USPS.

# 6. Client System Performance Criteria

The client system is defined as the processor running an appropriate software application that provides overall control of the mailpiece production process including the operator interface necessary for input of the parameters that are employed to customize the mailpiece (e. g., postage amount, date of mailing, destination ZIP Code, etc).

The core functions of the client system are configuration management, mailpiece production, communications management, log file and safe-store management, user interface, and user education and support. These functions are addressed in 6.1 - 6.6. Client system functions in support of the IBIP-specific functions (namely device authorization, finance, and indicia creation) are discussed in 6.7 through 6.9.

## 6.1. Configuration Management

The configuration management function ensures that the user's system configuration is current. Some of the functions of configuration management include configuring the client system for initial installation and setup, system modifications, and system uninstall; client system software update; and client system critical information update for the postal rate table USPS ZIP+4 National Directory CD-ROM, public-key certificates, and user profile.

The configuration management functions shall ensure the proper installation and configuration of the client system. The configuration management function shall ensure that updates and modifications to the client system are made in accordance with the performance criteria.

### 6.1.1. Client System Configuration

A client application, or a USPS-approved Provider procedure, shall be employed to ensure that the Client system configuration in use is current. Specifically, the system shall be configured for the underlying software and hardware, and all components shall have current USPS approval.

The major software components are the client system programs and the databases. The client system software shall have an identification number consisting of up to 12 digits. This number is the "Software ID" field included in indicium. See Chapter 3. The specific database components are the USPS Address Matching System (AMS), consisting of software and the ZIP+4 National Directory CD-ROM; the postal rates associated with the mailing classes and rate categories supported by the system; and the user profile, consisting of information from the user registration file and user system information. The client system shall verify the configuration to ensure that client system resident programs and critical information are as approved by the USPS and have not been modified.

#### **6.1.1.1.** Initial Installation and Setup

The client system shall provide functions and capabilities to allow the user to install client system software that is appropriately configured for the underlying software and hardware. The client system shall automatically detect, or query the user for, information regarding system resources and peripherals used by the client system. The client system

shall determine whether the available resources and devices satisfy the stated minimum configuration requirements. The client system shall determine whether the system can perform the essential functions of indicia preparation. During the installation process, the system shall verify the client can communicate with the PSD (i.e., the Provider infrastructure) and is able to send and receive information. Configuration and installation of the system may involve selecting device driver software appropriate for the specific devices and/or copying appropriate software components and data from the distribution media for incorporation in the client system.

**6.1.1.2.** System Modifications

The client system shall be capable of modifying the installation and configuration of the client system at the user's request or upon detecting substantive changes to the configuration. The client shall perform all necessary actions to change the configuration, including changing the Provider infrastructure records and updating user registration and user profile information, as appropriate for the configuration change. The client system shall have the capability to roll back to the previous configuration if it cannot confirm the integrity of an attempted configuration update.

**6.1.1.3.** Uninstall

The client system shall be capable of removing software and databases. The system shall provide the capability for either the user or the Provider infrastructure to initiate the uninstall function. Performing the uninstall function immediately after completing the install function should return the client system to its state prior to the install. If the uninstall function is invoked after at least one log file has been created, then the uninstall function should not delete any log files containing postage download or mailpiece creation records without first providing for the transmission of existing log files to the Provider infrastructure and then giving the user the opportunity to safe-store or retain the log files.

**6.1.1.4.** Client System Software Update

Upon each communication with the Provider infrastructure, the client system, through interaction with the Provider infrastructure, shall determine whether any changes to the client software configuration are required. If changes are required, they shall be made before producing any more indicia or increasing the postage value available. Acting under the direction of the Provider infrastructure, the client shall receive modifications from the Provider infrastructure and install them or else instruct the user regarding actions necessary to update the client configuration. If the software update mandates a resultant change to the software identification number, the change shall be made in the user profile.

**6.1.1.5.** Client System-Critical Information Update

The client shall ensure system-critical information is current. The critical information that shall be kept current includes the postal rate table, the USPS Address Matching System ZIP+4 Directory, and the user profile. Upon each communication with the Provider infrastructure, the client system, through interaction with the Provider infrastructure, shall

determine whether any system-critical information needs to be updated. If an update is required, it shall be made before producing any more indicia.

If the postal rate table is not current, the system shall either update the rate table or inform the user of any action necessary to obtain a current version. The Provider shall ensure that users have a reliable method of obtaining the new postal rate table before the current table expires.

If the USPS ZIP+4 National Directory is not current, the system shall either update the Directory or inform the user of any action necessary to obtain a current version. The Provider shall ensure that users have a reliable method of obtaining a new directory for the USPS ZIP+4 CD-ROM before the current directory expires.

The client shall maintain a user profile that contains critical information about the client installation and the responsible owner or user of the system. The user and installation information shall include, at a minimum, the information that the USPS requires in PS Form 3601-A, *Application or Update for a Registration to Lease and Use Postage Evidencing Systems*, the information returned with PS Form 3601-B, *Registration to Lease and Use Postage Evidencing Systems*, as well as the software identification number and the PSD serial number.

### 6.2. Mailpiece Production

The mailpiece production function of the client system is responsible for generating the elements of a properly formatted mailpiece front, including the USPS-approved indicium, the FIM (when required, a valid delivery address, and a POSTNET barcode (where required. These elements shall be formatted and positioned on the mailpiece or label in accordance with USPS requirements.

#### 6.2.1. Standard Services

The client shall produce the mailpiece front, including the delivery address, the POSTNET barcode (when required), the FIM (when required), and the indicium, as an integral unit. The client may print this unit on the actual mailpiece stock or on label(s) for later attachment to the mailpiece. The client shall indicate to the user when the FIM is required on the mailpiece, but shall also provide the user with an option to omit the FIM when the FIM is preprinted on the mailpiece, when it is not required for the given mail class, or when it is not required for another reason

For mail with a domestic destination, the location of the various mailpiece components (indicium, POSTNET barcode, delivery address, and FIM) and the overall appearance of the mailpiece shall comply with the requirements in the DMM and Publication 25, *Designing Letter Mail*, for the given class of mail and size of mailpiece. For mail with an international destination, the overall appearance of the mailpiece shall comply with the requirements in IMM 145.3 for the given class of mail and size of mailpiece.

[2] The Postal Service is developing policies, procedures, and systems that will distinguish between postage meter and IBI postage evidencing systems.

The indicium component of the mailpiece shall comply with the performance criteria for the indicium as given in Chapter 3. The user shall print only a USPS-authorized indicium that has been preapproved by the manager of Postage Technology Management.

A complete and accurate date shall be printed on the mailpiece. The client system shall not allow mailpiece generation with a mailing date earlier than the current calendar date. The date of the indicium shall represent the actual date of deposit of the mailpiece. In some cases, a correction of the date may be needed. See Chapter 3 for the criteria for the redate indicium.

A mailpiece may be generated with a date of mailing in the indicium not exceeding 30 days in advance of the date on which the mail is to be deposited with the Postal Service. The client system shall ask the user to actively acknowledge a notification that mail will not be accepted by the Postal Service prior to the mailing date in the indicium when that date is more than 1 day in advance of the date of deposit of the mailpiece.

For domestic mail the client shall integrate and use the USPS Address Matching System (AMS) Application Program Interface (API) to produce a standardized address for the mailpiece. The client may perform the ZIP+4 validation at the time of indicia creation or may provide another method that satisfies USPS requirements for the proper ZIP+4 coding. The standardized address shall include the standard POSTNET delivery point barcode.

For mail with an international destination, the formats of the origination and destination addresses are in accordance with IMM 122.

### 6.2.2. Expedited and Special Mail Services

The client system shall assist the user in the preparation of mailpieces that take full advantage of expedited and special mail services Expedited services include Express Mail, Priority Mail, International Express Mail, Global Priority Mail, and Priority Mail Global Guaranteed. Special services include Certified Mail, delivery confirmation, and other services, as they become available.

In addition to preparing the indicia to indicate payment for expedited and special mail services, the client system shall complete the special forms for these products, including the generation of a one-dimensional barcode and a tracking number. The USPS will supply the allowable tracking numbers to the Provider. The format of the special forms and generation of the tracking information will be addressed in a future version of this document.

## 6.3. Communications Management

The communications management function is responsible for relaying messages between the client system and the Provider infrastructure. This includes the Indicia Request Message (IRM), the PSD Response Message (PSDRM), any initial log-on messages, any messages required to support configuration management, and the transmission of any log files. The selection of the transmission media and security protocol is left to the Provider.

If the given system supports the ability to obtain or maintain a user registration through the client system, communications shall be provided to support that function as well. Communications involving user registration require strong identification and authentication of the client to the Provider infrastructure, and of the Provider infrastructure to the client. The client system shall implement effective communication between the user and the Provider infrastructure. The client system shall select the connection method from those supported by the USPS as part of the initial system setup and subsequently establish the communications channel as needed to support the functions described in these performance criteria

The client system shall be designed to recover from communications failures that could occur at any point in the process, including any supporting interaction between the USPS and the Provider infrastructure. Possible actions to take when a failure occurs include restart or rollback. In the event of lost communications, and if communications cannot be reestablished during the current user session, the client system shall be capable of returning the system to the state existing at the time of the interruption.

### 6.4. Log File and Safe Store Maintenance

The log file and safe-store maintenance function of the client system shall maintain log files with entries relating to user activity and shall provide a safe-store function to protect selected, critical information against loss. The log files record use of the system and provide automated records containing information required by the USPS. The safe-store function involves creating copies of critical information, including log files, that can survive catastrophic system failures.

The client shall maintain a log file that records significant events. All transactions relating to indicia creation or funds transfer must be logged. Additional events may be logged at the Provider's discretion. The client system shall provide for automatic transmission of log files from the client system to the Provider infrastructure. The client system shall also provide a capability to safe-store information. The log file must be designed to prevent easy access from any software other than the client system. The following sections detail the fields required for each of the required log file entries.

#### 6.4.1. Funds Transfer Log File Entry

An entry shall be made to the log file to record each purchase of postage by the user. The postage transfer message, showing the transaction amount, shall be included in the entry. The entry shall contain a result code that indicates whether the transfer succeeded or failed and the reason(s) for any failure.

#### 6.4.2. Indicia Creation Log File Entry

An entry shall be made to the log file to record each indicium created. Table 6-1, Indicia Creation Log File Entry, shows that the required fields are a subset of those required for the indicium, with some additional identifying information. The order and formatting of this data are defined in Table 6-1.

**Table 6-1. Indicia Creation Log File Entry**

| Fields | Format or Value | | | |
|---|---|---|---|---|
| Date and Time of Indicia Creation | YYYYMMDD/HH:mm:SS | | | |
| Log Entry Type (A log file entry for the redate indicium is optional | Standard Indicia 07 | Postage Correction 08 | Redate Indicia 09 | Refund Indicia 10 |
| Indicia Version Number | ASCII, 1 character | | | |
| Algorithm ID | ASCII, 1 character | | | |
| Certificate Serial Number | Alphanumeric, 9,999,999,999 | | | |
| PSD Device ID:<br>Manufacturer ID<br>Model ID<br>Serial Number | <br>Alphanumeric, 2 characters<br>Alphanumeric, 2 characters<br>Numeric, 10 digits | | | |
| Ascending Register | Numeric, 999,999,999.999 | | | |
| Postage | Numeric, 99.999 | | | |
| Date of Mailing | YYYYMMDD | | | |
| Originating Address (Registration ZIP Code) | Alphanumeric, 99999 | | | |
| Destination Delivery Point 5-digit ZIP Code | Alphanumeric, 99999-0000 (This field has zero value for correction indicia and international mail | | | |
| Software ID | Numeric, 12 digits | | | |
| Descending Register | Numeric, 999,999.999 | | | |
| Rate Category | Numeric, 4 digits | | | |

### 6.4.3. Log File Management and Review

The client system shall provide capabilities to create new log files, safe-store log files, and view log files. The log files shall be assigned names in the underlying system file structure to provide insight into the sequence of log entries across multiple files. The log file must be designed to prevent the user from directly manipulating the log file entries. The client system shall provide an automated means to transmit log file entries to the Provider's infrastructure with every connection, including the connection for transmittal of the refund request indicium. Only those entries not previously transmitted, rather than the entire contents of the log file, need to be transmitted. It is the responsibility of the client system to maintain accurate records of which entries have been transmitted. Once each Postal Accounting period, the Provider shall submit to the Postal Service infrastructure all user log files not previously transmitted.

### 6.4.4. Safe-Store

The client system shall provide a capability to safe-store information. Critical information that is necessary for the operation of the system, and is not otherwise recoverable, shall be safe-stored when created or updated. Following a catastrophic hardware or software failure, an inadvertent accident, or any loss or detected corruption, the client system shall be able to restore information that has been safe-stored Information shall be safe-stored by making copies on storage media that may be removed and physically separated from the client system, or by copying the information to a remote location accessible over a network.

### 6.5. User Interface

User interface functions shall allow the user to control and operate the system, obtain status information, and perform quality assurance functions. The user interface may also provide the means for the user to apply for and update user registrations and leases.

The client system shall provide an interface to allow the user to initiate, control, and interact with the functions and operations described in these performance criteria. The user interface should comply with standard human engineering practices and should prompt and help users to provide complete, accurate input data. The client should provide informative responses that clearly indicate the success or failure of each request. Error messages should inform the user clearly of the nature of the error and the corrective action required. The remaining paragraphs describe additional interface requirements.

#### 6.5.1. General Information Displays

The client system shall provide the user with the means to request information on the current status of the client system. The information the client shall provide to the user is listed in Table 6-2. The client may offer several displays that collectively provide the indicated information.

**Table 6-2. Information Display Items**

| Information Display Items |
|---|
| Device ID/Type |
| Cumulative Postage (Ascending Register) |
| Remaining Postage (Descending Register) |
| User Registration Application Information, including Registration Number |
| Current Rate Table Version |
| Current AMS ZIP+4 CD-ROM Version |
| Software ID Number |
| Provider Name and Contact Information |

#### 6.5.2. Advisory Messages

During user interaction with the functions and operations of the system, the client system shall report to the user any errors that occur. Such errors include having insufficient postage available to print the requested indicium or requesting a postage amount for the indicium that is out of the allowable range.

#### 6.5.3. Indicia Quality Assurance

Periodically, the client shall produce indicia for Provider review and quality assurance. The user interface shall instruct the user to mail the quality assurance indicium to the Provider. The Provider shall inspect the indicium for compliance with USPS policy and IBIP requirements to ensure that the indicium components are readable and properly oriented and positioned The Provider shall inform users of any problems found and advise them of corrective action they need to take.

The first quality assurance indicium shall be produced for Provider review in conjunction with the initial installation of the system. It shall be produced after completion of the

product initialization and authorization and after obtaining a user registration. Subsequently, the schedule for production of the quality assurance indicia shall be as required by the USPS.

### 6.5.4. Postage Evidencing System Lease and User Registration Application and Update[3]

If the client system provides the means to request or update a registration for use of a postage evidencing system, the client shall collect the required information in accordance with requirements of the USPS Centralized Registration System (CRS). If the client system does not provide the means to request or update the postage evidencing system user registration, it is the Provider's responsibility to ensure that the user registration information is accurate and complete prior to producing indicia.

The client shall print a hardcopy of the lease for appropriate signature and instruct the user to mail the signed document to the Provider In lieu of a hardcopy lease, the client may allow the user to actively acknowledge the terms and conditions of an electronic service agreement, and to transmit the acceptance to the Provider infrastructure using a process that authenticates the user. The terms and conditions of the electronic service agreement must be approved by the USPS before implementation.

The client shall provide the user a copy of any USPS privacy policy applicable to IBI products. The Provider is responsible for ensuring the user reads and actively accepts the conditions of any privacy policy prior to producing indicia.

## 6.6. User Education and Support

The user education and support function provides users with information on how to use and operate the system and informs them of their responsibilities with respect to the use of IBI.

The client system, or supporting documentation, shall provide training and support material to allow users to install and operate the system without assistance. The training and support shall include the USPS's general rules for IBI use and related federal laws and their consequences. The training material should highlight the proper position and location for the indicium and other elements of mailpiece design, especially the FIM (when required). The Provider may use or reproduce existing USPS materials intended for IBI users. It is recommended that an on-line help file be included for the user as part of the client system.

## 6.7. Device Authorization

The client system provides the interface to the Provider's infrastructure (i.e., the PSD) for loading user-specific information for device authorization, in accordance with the performance criteria in Chapter 4. The client system also provides the interface to the Provider's infrastructure (i.e., the PSD) for updating the device authorization information with all relevant changes to the user profile or other authorization information.

---

[3] The Postal Service is developing policies, procedures, and systems that will distinguish between postage meter and IBI postage evidencing systems.

### 6.8. Finance

The client system finance function includes the electronic transfer of funds to the USPS Treasury for subsequent representation of the amount paid in an equal amount of postage reflected in the user's revenue sensitive registers. The client system finance function also allows the user to obtain a refund of the remaining postage value when the PSD is withdrawn from service.

#### 6.8.1. Obtaining Postage

The client system shall provide or direct the user to information on how to transfer funds to the USPS for postage. The client system shall enable the user to verify the amount. The client system may provide the user with the necessary functions to transfer funds electronically to the USPS. The need for and nature of these payment functions is dependent on the Provider business model and USPS policy.

#### 6.8.2. Remaining Postage Value Refund

The client system shall provide the interface between the user and the Provider infrastructure for the refund of remaining postage value. The user can obtain a refund of postage value in the PSD only when the PSD is withdrawn from service. The refund request must be for the entire postage value remaining in the PSD, as shown on the descending register at the initiation of the refund process. There shall be no mechanism for processing a partial refund of an amount remaining on the PSD. The request for postage value refund shall be the last transaction permitted for the PSD.

The user initiates the request for a refund through the client system. The client system verifies the amount of postage remaining on the PSD and collects the data required for transmission of the refund request to the Provider. The data integrity requirements for this refund request consist of the following:

- The refund request message shall be digitally signed by the user using a USPS approved "Public-Key" algorithm (sometimes referred to as an asymmetric algorithm) with a private key unique to that user. This key is denoted by $V_{CUST}$.
- The signature on the refund request message, upon receipt by the PSD, shall be verified using the corresponding public key of the user, $U_{CUST}$.

The Provider is responsible for collecting any additional data required to process the refund. The format of the refund request message shall be left up to the creativity of the Provider, but it is subject to USPS approval.

The Provider infrastructure is responsible for verifying the postage value refund request and for issuing a refund to the individual user. On a regular basis, the Provider will submit to the Postal Service an aggregate total of all refunds issued to users. The Postal Service will issue a refund to the Provider for the aggregate total of all refunds for unused postage or for postage value remaining on the PSDs that were issued by the Provider during the period covered. The Provider is required to maintain documentation supporting all individual refunds to users for periodic Postal Service audits.

### 6.9. Indicia Creation

The client system shall create indicia and transmit indicia to the printer. The client system shall provide the PSD with the mailpiece-specific data elements necessary to prepare the indicia and the mailpiece (i.e., the customization data). The client system shall prevent the printing of multiple copies of an indicium, and shall restrict printing to only one image.

The client shall provide the capability to produce and print four types of indicia: the standard indicium, the date correction indicium, the postage correction indicium, and the test indicium. Chapter 3 provides specific detailed requirements regarding the content, position, readability, and print characteristics for the standard, date correction, and postage correction indicia.

#### 6.9.1. Date Correction and Postage Correction Indicia

The client shall be capable of producing date correction and postage correction indicia. The client shall be capable of printing these indicia on either the non-addressed side of the mailpiece or on a label that will be affixed to the mailpiece, in accordance with the requirements of the DMM. The client shall produce the date correction indicium without employing the PSD.

The production of the postage correction indicium does require use of the PSD. The data elements to be included in the postage correction indicia are found in Chapter 3. The client shall provide the data elements to the PSD to produce the additional postage value and to digitally sign the indicia.

#### 6.9.2. Test Indicia

The client shall be capable of producing test indicia. The client must produce the test indicia without employing the PSD. The user generates a test indicium to verify location of the indicium on the mailpiece and to check on print quality and other aesthetic features prior to printing valid indicia. The test indicium shall clearly indicate it is not usable as evidence of postage. There are no other specific performance criteria associated with the test indicium

# 7. KEY MANAGEMENT PERFORMANCE CRITERIA

Digital signatures based on public-key cryptography are required in the IBIP for the creation of the indicium, in accordance with the performance criteria in Chapter 3 and Chapter 4. This approach relies on a pair of cryptographic keys, a private key, and a public key. The private key is used by the signatory for creating the signature. The recipient uses the public key for verifying that signature. Multiple digital signature algorithms are supported by the IBIP (see Chapter 4). A Provider is at liberty to choose the digital signature algorithm(s) most appropriate for its product(s).

IBIP uses X.509 Version 3 certificates as the vehicle for distributing the necessary cryptographic keys to the IBIP elements requiring them. The IBIP Certificate Authority (CA) is responsible for the creation and distribution of these certificates.

A USPS-supplied interface supports the IBIP key infrastructure for Providers. The IBIP key infrastructure services (which include trust evaluation, key registration and key selection, key distribution, and certificate revocation) support the applications of public-key cryptography to the IBIP for Open Systems. The IBIP standard is based on the use of X.509 certificates. The USPS will supply all qualified IBI Providers with additional details of the key interface and of the key management plan.

## 7.1. Key Registration

This section describes the IBIP trusted keying hierarchy, the generation of the certificates for the Provider, and the PSD certificate registration procedure.

### 7.1.1. IBIP Trusted Hierarchy

There are four IBIP entities that use digital signatures and require cryptographic keys and digital signature certificates, namely the CA, the USPS IBIP Registration Authority (RA), the Providers, and the PSDs. The certificates are required to verify the indicia objects issued by each authorized PSD.

IBIP has a single CA. The organization of the IBIP trusted keying hierarchy, based on the public-key certificates, is depicted in Figure 7-1.

The CA generates and distributes the CA Certificate to the first level of the keying hierarchy, the USPS IBIP RA. The USPS IBIP RA must authenticate the IBIP Provider to the CA before the CA generates a certificate for the second level of the keying hierarchy (the Provider). The IBIP Provider, in turn, authenticates each PSD to the CA. The CA then generates a certificate that is transmitted through the Provider to the third level of the keying hierarchy (the PSDs).

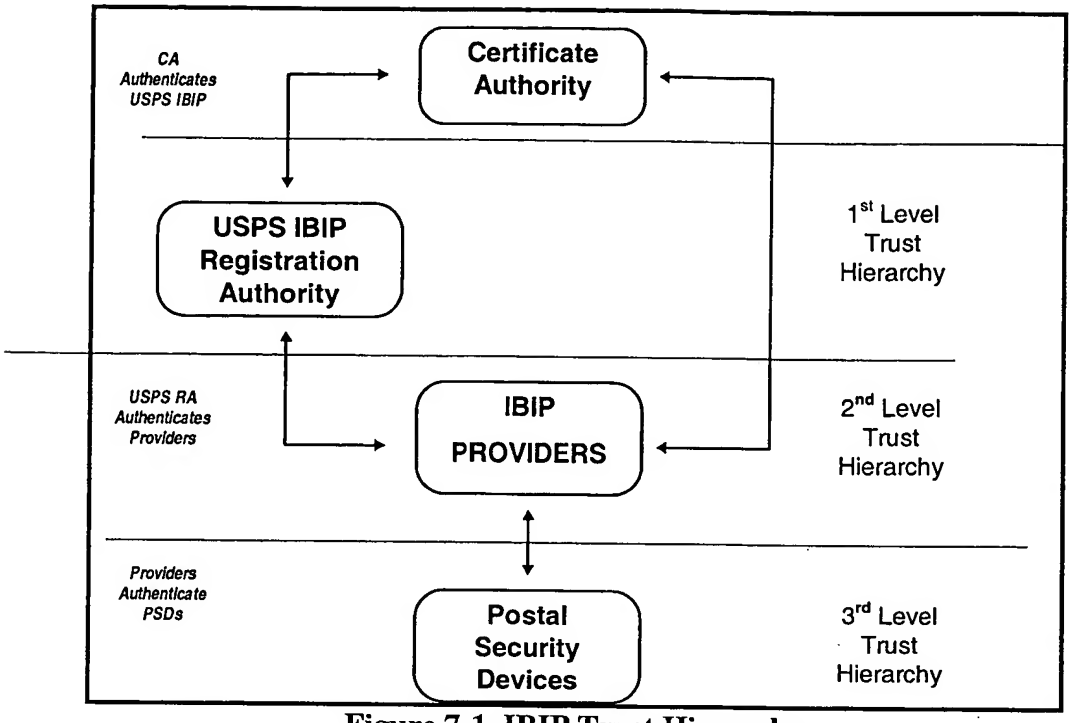



**Figure 7-1. IBIP Trust Hierarchy**

### 7.1.2. Provider Certificate Registration Procedure

Before a Provider can request certificates for its PSDs, it must have its own Provider certificate. The Provider receives its certificate from the IBIP RA. As part of the process for obtaining this certificate:

- The IBIP RA authenticates the identity of the Provider's representative.
- The IBIP RA generates the key pair.
- The IBIP RA submits a certificate request to the CA for the Provider.

The USPS conducts this process in the presence of the Provider. The Provider's private key is stored on a token selected by the USPS. This token is used to sign the PSD certificate requests. All software or tool kits required to perform this function are provided by the USPS.

### 7.1.1. PSD Certificate Registration Procedure

Once the Provider receives its token, the Provider may thereafter request certificates for its PSDs from the CA. This process can be accomplished in one of the following ways:

- The Provider uses the USPS-supplied single-request registration authority application.
- The Provider develops an application using the USPS-supplied IBIP Public-Key Infrastructure application program interface (API).

For both of the methods described above, the Provider signs the PSD certificate requests with the token obtained during the Provider certificate registration procedure and receives

an X.509 certificate in return. The actual implementation and data requirements for the certificate request are beyond the scope of this document but will be supplied to qualified Providers.

### 7.1.4. Other Certificate Procedures

The PSD certificate discussed in 7.1.3 is the certificate associated with the indicia signature creation and indicia signature verification key pair (i.e., those identified as $V_{PSD}$ and $U_{PSD}$ in previous portions of this document). However, other key pairs (also identified in this document) also require certificates. They are the IRM signature creation and IRM signature verification key pair identified by $V_{CUST}$, $U_{CUST}$, and, if used (as opposed to using a secret key algorithm), the PSDRM encryption key and PSDRM decryption key identified by $V_{PSDRM}$ and $U_{PSDRM}$. It is left to the Provider to develop a methodology for obtaining and distributing these other certificates. Any methodology developed is subject to approval by the USPS.

## 7.2. Key Attributes

Attributes for the public keys in the algorithms currently approved for use in the IBIP (namely DSA, RSA, and ECDSA) are described in 7.2.1 through 7.2.3 along with the key attributes for the keys necessary to perform the cryptography specified in this document between the user and the Provider.

### 7.2.1. Key Lengths

The key length, in bytes, for each of the key uses is shown in Table 7-1.

**Table 7-1. Key Lengths**

| Key Use | Key Length (bytes) |
|---|---|
| Indicia Signature Key | For DSA/RSA, length = 128<br>For ECDSA, length = 20 |
| Indicia Request Message (IRM) Key | For DSA/RSA, length = 128<br>For ECDSA, length = 20 |
| PSD Response Message Encryption (PSDRM) Key | For DSA/RSA, length = 128<br>For ECDSA, length = 20<br>For Secret Key Algorithm, length = 16 |

### 7.2.2. Cryptoperiods

The cryptoperiod of a key is the length of time for which that key is valid. The cryptoperiods established by the USPS for the various IBIP entities are shown in Table 7-2.

**Table 7-2. IBIP Cryptoperiods**

| IBIP Entity | Cryptoperiod |
|---|---|
| USPS IBIP Element / Provider Keys | 3 years |
| Postal Security Device Keys, $V_{PSD}$ | 3 years |
| IRM Keys, $V_{CUST}$ | 3 years |
| PSDRM Keys, $V_{PSDRM}$ (if used) | 3 years |
| PSDRM Secret Encryption Key, $K_{PSDRM}$ | Changed on a per session basis (in no case shall a session exceed 24 hours) |

When the cryptoperiod expires, a new certificate (containing a new key) must be created and distributed.

### 7.2.3. Additional Attributes

The USPS will make additional details of IBIP key management available to all qualified Providers.